NetComm®
www.netcomm.com.au

User Guide

NB6, NB6W, NB6Plus4W

ADSL2+ Modem Router

Safety and Precaution

Installation

- Use only the type of power source indicated on the marking labels.
- Use only power adapter supplied with the product.
- Do not overload wall outlet or extension cords as this may increase the risk of electric shock or fire. If the power cord is frayed, replace it with a new one.
- Proper ventilation is necessary to prevent the product overheating. Do not block or cover the slots and openings on the device, which are intended for ventilation and proper operation. It is recommended to mount the product with a stack.
- Do not place the product near any source of heat or expose it to direct sunlight.
- Do not expose the product to moisture. Never spill any liquid on the product.
- Do not attempt to connect with any computer accessory or electronic product without instructions from qualified service personnel. This may result in risk of electronic shock or fire.
- Do not place this product on unstable stand or table.

When in Use

- Power off and unplug this product from the wall outlet when it is not in use or before cleaning. Pay attention to the temperature of the power adapter. The temperature might be high.
- After powering off the product, power on the product at least 15 seconds later.
- Do not block the ventilating openings of this product.
- When the product is expected to be not in use for a period of time, unplug the power cord of the product to prevent it from the damage of storm or sudden increases in rating.

Service

Do not attempt to disassemble or open covers of this unit by yourself. Nor should you attempt to service the product yourself, which may void the user's authority to operate it. Contact qualified service personnel under the following conditions:

- If the power cord or plug is damaged or frayed.
- If liquid has been spilled into the product.
- If the product has been exposed to rain or water.
- If the product does not operate normally when the operating instructions are followed.
- If the product has been dropped or the cabinet has been damaged.
- If the product exhibits a distinct change in performance.

Caution

- Any changes or modifications not expressly approved by the party responsible for compliance could void the authority to operate equipment.

Copyright Notice

* 2005 All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of the seller.

Disclaimer

Information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. The seller therefore assumes no responsibility and shall have no liability of any kind arising from the supply or use of this document or the material contained herein.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, the seller reserves the right to make changes to the products described in this document without notice.

The seller does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Trademarks

All other product or service names mentioned in this document may be trademarks of the companies with which they are associated.

Contents

Before You Use 6
NB6 Series Package Contents 7
Features 8
ADSL Compliance 8
ADSL2 Compliance 8
ADSL2+ Compliance 8
Wireless LAN Compliance 8
ATM Features 9
Bridging Features 9
Routing Features 9
Security Features 10
Configuration and Management 10
Subscription for ADSL Service 10
Chapter 1: Overview 11
Physical Outlook 12
NB6 LED Indicators 12
NB6 Rear Panel 13
NB6W LED Indicators 14
NB6W Rear Panel 15
NB6Plus4W LED Indicators 16
NB6Plus4W Rear Panel 17
Chapter 2: System Requirement and Installation 18
System Requirement 18
Do I need a Micro Filter 19
Choosing a place for the ADSL Router 20
Connecting the ADSL Router 20
USB Driver Installation 21
For Windows ME 21
For Windows 2000 21
For Windows XP 22
Uninstalling the USB Driver 24
For Windows ME 24
For Windows 2000 24
For Windows XP 25
Setting up TCP/IP 26
For Windows 98 26
For Windows ME 26
For Windows NT 27
For Windows 2000 27
For Windows XP 28
Renewing IP Address on Client PC 32
For Windows 98/ME 32
For Windows NT/2000/XP 32

Chapter 3: Accessing the Internet....33
PPP over ATM (PPPoA) Mode....34
PPP over ATM (PPPoA) IP Extension Mode....35
PPP over Ethernet (PPPoE) Mode....36
PPP over Ethernet (PPPoE) IP Extension Mode....37
Numbered IP over ATM (IPoA)....38
Numbered IP over ATM (IPoA)+NAT....39
Unnumbered IP over ATM (IPoA)....40
Unnumbered IP over ATM (IPoA)+NAT....41
Bridge Mode....42
MER....43
Chapter 4: Web Configuration....44
Using Web-Based Manager....44
Outline of Web Manager....45
To Have the New Settings Take Effect....45
Language....45
Quick Start....46
Connect to Internet....46
Quick Setup....47
Connection Type....48
PPP over ATM/ PPP over Ethernet....49
IP over ATM....52
Bridging....55
Status....58
Overview....59
ADSL Line....58
Internet Connection....60
Traffic Statistics....60
DHCP Table....61
Wireless Clients....61
Routing Table....61
ARP Table....61
Advanced Setup....62
Local Network – IP Address....62
Local Network – DHCP Server....64
Local Network – UPnP....66
Local Network – IGMP Snooping....67
Internet – Connections....69
Internet – DNS Server....74
Internet – IGMP Proxy....75
Internet – ADSL....76
IP Routing – Static Route....77
IP Routing – Dynamic Routing....79
Virtual Server – Port Forwarding....80
Virtual Server – Port Triggering....84
Virtual Server – DMZ Host....85
Virtual Server – Dynamic DNS....86

Virtual Server – Static DNS 87
Firewall 88
Firewall – IP Filtering 89
Quality of Service 92
Quality of Service – Bridge QoS 92
Quality of Service – IP QoS 94
Port Mapping 97
Wireless 100
Basic 100
Security 103
Access Control 111
Repeater 113
Management 115
Diagnostics 115
Management Accounts 117
Management Control – From Remote 118
Management Control – From Local 119
Internet Time 120
System Log 121
SNMP Setting 125
Backup Config 127
Update Firmware 129
Reset Router 129
UPnP for XP 130
Chapter 5: Troubleshooting 132
Problems with LAN 132
Problems with WAN 132
Problems with Upgrading 133
Chapter 6: Glossary 134
Appendix A: Client Setup for 802.1x, WPA, and WPA-PSK 136
Retreiving Client Certificate 136
Enabling 802.1x Authentication and Security 139
Enabling WPA Authentication and Security 144
Enabling WPA-PSK Authentication and Security 147
Appendix B: Legal and Regualtory Information 149
Customer Information 149
Product Warranty 150
Limitations of Warranty 150

BEFORE YOU USE

Thank you for purchasing a NetComm ADSL2+ Modem Router. NetComm brings you the Next Generation of ADSL technology with ADSL2+*, which boosts ADSL's performance, improves interoperability, and supports new applications, services and deployment conditions.

NetComm's implementation of ADSL2+* ensures that your Modem Router operates with existing ADSL services while delivering optimal performance in all modes of operation. Powered by the latest Broadcom ADSL+2* chipset, NetComm's Modem Router provides downstream data rates of up to 24Mbps in ADSL2+* mode ensuring that you can surf the net or download your files quicker than ever before.

Security is a key issue with Broadband users and NetComm's Modem Routers do not leave you exposed. Your new Modem Router has a built-in firewall to ensure your defences are rock-solid against hackers, unauthorised entries, probes and even Denial of Service attacks. What's more, your Modem Router is equipped with a VPN pass-through feature allowing you to use a standard VPN client for Point-to-Point communication even while your Firewall is active.

NetComm's NB6 Series Modem Routers deliver the connection versatility needed to cater for today's ADSL users. Simply attach to a single PC using the Ethernet port (recommended) or USB port. Alternatively, should you wish to share your Internet connection, the Modem Router is equipped with an in-built Router and one or four Ethernet ports for connection to a network. If you have the NB6W or NB6Plus4W modem, you can also share your Internet connection wirelessly.

The Modem Router's Port Forwarding and UPnP functions have made it easier for today's Internet users to configure and setup the myriad of Network Port Rules needed by Internet applications such as On-Line Gaming, Peer-To-Peer file sharing and Messenger services to operate. The Modem Router has a number of pre-configured rules for several games, just click on the game you wish to play on-line and the rest is done for you.

Added to this, the Modem Router introduces a QoS (Quality of Service) feature that gives you control over which types of data are given priority by the Modem Router.

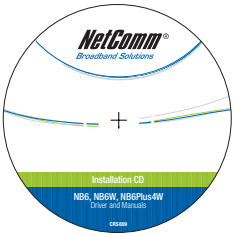
* *Your ISP must support and provide you with an ADSL-2 or ADSL-2+ service for these features to be available. This product will operate as a standard ADSL Modem Router when an ADSL-2 service is not available.*

This reference manual assumes that the reader has an installed Ethernet card in the computer to be connected and has basic to intermediate computer and Internet skills. However, basic Computer Networking, Internet, and Firewall technology information is available from the NetComm Web site. See www.netcomm.com.au.

NB6 Series Package Contents

Your Package contains the following items:

- One NB6, NB6W, NB6Plus4W Modem Router (all models shown above)



- Driver and Manual CD

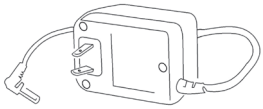
- One Quick Start Guide

If any of the above items are damaged or missing, please contact NetComm immediately.

- Telephone Cable (RJ-11)

- USB Cable

- CAT-5 UTP Straight Ethernet Network Cable (RJ-45)



- Power Adaptor (NB6 - 9V AC 1A, NB6W/NB6Plus4W - 12V AC 1A)

Features

ADSL Compliance

- ANSI T1.413 Issue 2
- ITU G.992.1 Annex A (G.dmt)
- ITU G.992.2 Annex A (G.lite)
- ITU G.994.1 (G.hs)
- Support dying gasp
- Maximum Rate: 8 Mbps for downstream and 1 Mbps for upstream

ADSL2 Compliance

- ITU G.992.3 Annex A (G.dmt.bis)
- Maximum Rate: 12 Mbps for downstream and 1 Mbps for upstream

ADSL2+ Compliance

- ITU G.992.5 Annex A (G.dmt)
- Maximum Rate: 24 Mbps for downstream and 1.2 Mbps for upstream

Wireless LAN Compliance (NB6W and NB6Plus4W only)

- IEEE 802.11g and IEEE 802.11b
- Data Rate: 54, 48, 36, 24, 18, 12, 9, 6 Mbps for 802.11g; 11, 5.5, 2, 1 Mbps for 802.11b
- Modulation Technique: OFDM for 802.11g; CCK (11 Mbps, 5.5 Mbps) for 802.11b; DQPSK (2Mbps) for 802.11b; DBPSK (1 Mbps) for 802.11b
- Network Architecture: infrastructure
- Operating Frequency: 2.4 ~ 2.5 GHz
- Operating Channels: depending on local regulations. For example, 11Channels (Northern America), 13 Channels (Europe), and 14 Channels (Japan)
- RF Output Power: 13.5+/-1.5dBm for 802.11g; 17.5+/-1.5dBm for 802.11b
- Antenna Connectors: Hardware diversity support. One external antenna and one internal antenna are provided (both are fixed and cannot be changed).
- Coverage Area: 300 meters
- Support WEP (Wired Equivalent Privacy) mechanism which uses RC4 with 64-bit or 128-bit key length
- Support 802.1x and WPA/WPA2
- Support the Access Control function: only registered WLAN clients are allowed to associate to this device.
- SSID can be hidden for the security issue (Don't broadcast SSID).
- Support the Repeater function to extend the coverage area
- Support wireless user isolation for the hotspot

ATM Features

- Compliant to ATM Forum UNI 3.1 / 4.0 Permanent Virtual Circuits (PVCs)
- Support up to 16 PVCs for UBR, CBR, VBR-nrt, VBR-rt with traffic shaping
- RFC2684 LLC Encapsulation and VC Multiplexing over AAL5
- RFC2364 Point-to-Point Protocol (PPP) over AAL5
- RFC2225 Classical IP and ARP over ATM
- RFC2516 PPP over Ethernet: support Relay (Transparent Forwarding) and Client functions
- Support PPPoA or PPPoE Bridged mode (the IP address got from ISP can be passed to the user's PC and behave as the IP address of the user's PC.)
- OAM F4/F5 End-to-End/Segment Loopback Cells

Bridging Features

- Supports self-learning bridge specified in IEEE 802.1d Transparent Bridging
- Supports up to 4096 learning MAC addresses
- Transparent Bridging among 10/100 Mb Ethernet, USB, and 802.11g wireless LAN
- Supports IGMP Snooping
- Supports 802.1Q VLAN packet pass-through

Routing Features

- NAT (Network Address Translation) / PAT (Port Address Translation) let multiple users on the LAN to access the internet for the cost of only one IP address.
- ALGs (Application Level Gateways): such as NetMeeting, MSN Messenger, FTP, Quick Time, mIRC, Real Player, CuSeeMe, VPN pass-through with multiple sessions, etc.
- Port Forwarding: the users can setup multiple virtual servers (e.g., Web, FTP, Mail servers) on user's local network.
- Support DMZ
- UPnP IGD (Internet Gateway Device) with NAT traversal capability
- Static routes, RFC1058 RIPv1, RFC1723 RIPv2
- DNS Relay, Dynamic DNS
- DHCP Client/Relay/Server
- Time protocol can be used to get current time from network time server
- Support IGMP Proxy
- Support port mapping function which allows you to assign all data traffic transmitted among specific Internet connections and LAN ports
- Support IP/Bridge QoS for prioritize the transmission of different traffic classes
- Support 802.1Q VLAN Tagging

Security Features

- PAP (RFC1334), CHAP (RFC1994), and MS-CHAP/MS-CHAP2 for PPP session
- Firewall support IP packets filtering based on IP address/Port number/Protocol type
- Support DoS (Deny of Services) which detect & protect a number of attacks (such as SYN/FIN/RST Flood, Smurf, WinNuke, Echo Scan, Xmas Tree Scan, etc)

Configuration and Management

- User-friendly embedded web configuration interface with password protection
- Remote management accesses control
- Telnet/SSH session for local or remote management
- Firmware upgrades through HTTP, TFTP, or FTP
- The boot loader contains very simple web page to allow the users to update the run-time firmware image.
- Configuration file backup and restore
- SNMPv1/v2 agent with MIB-II, ADSL Line MIB

Subscription for ADSL Service

To use the ADSL Router, you have to subscribe to an ADSL service from your broadband service provider. According to the service type you select, you may get various IP addresses:

Dynamic IP:	If you apply for an on-demand connection, you will be given an Internet account with username and password. You will get a dynamic IP issued by your ISP, such as under PPPoA, PPPoE, or MER mode.
Static IP address:	If you apply for full-time connectivity, you may get either one static IP address or a range of IP addresses from your ISP. The IP address varies according to different ADSL service provider, such as using IPoA or MER mode.

CHAPTER 1: OVERVIEW

This chapter provides you with a description for the LEDs and connectors on the front and rear surface of the router. Please take a look at this information, before you use/install this router.

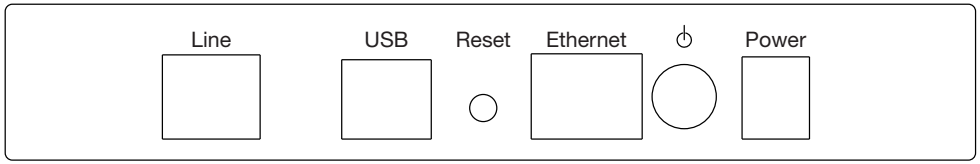
NB6 LED Indicators

The LED Indicators are located on the front of the unit, their meanings are as follows:

Function	Color	Definition
Power	Off	Power is off.
	Solid Green	Power is on and the device operates normally.
	Solid Red	Power on self-test in progress
		The device enters the console mode of the boot loader.
		Power on self-test failure if the led always stays solid red.
	Flash Red	Firmware upgrades in progress
ADSL	Off	No ADSL signal is detected.
	Slow Flash Green	ADSL line is handshaking in progress
	Fast Flash Green	ADSL line is training in progress
	Solid Green	ADSL line connection is up.
PPP	Off	No PPPoA or PPPoE connection
	Solid Green	At least one PPPoA or PPPoE connection is up. The users can access the Internet now.
Ethernet	Off	No Ethernet signal is detected.
	Flash Green	User data is going through Ethernet port
	Solid Green	Ethernet interface is ready to work.
USB	Off	No USB signal is detected.
	Flash Green	User data is going through USB port
	Solid Green	USB interface is ready to work.

NB6 Rear Panel

The following figure illustrates the rear panel of your ADSL Router:



Connector	Description
Line	RJ-11 connector (Telephone line)
USB	USB connector
Reset	Reset to factory defaults
Ethernet	Ethernet RJ-45 connector
⏻	Power on/off switch
Power	9VAC Power connector

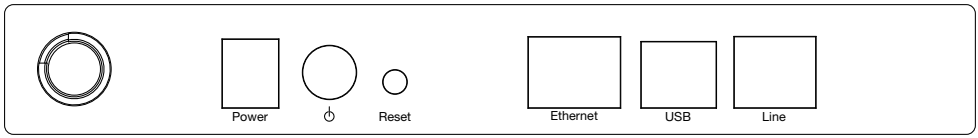
NB6W LED Indicators

The LED Indicators are located on the front of the unit, their meanings are as follows:

Function	Color	Definition
Power	Off	Power is off.
	Solid Green	Power is on and the device operates normally.
	Solid Red	Power on self-test in progress
		The device enters the console mode of the boot loader.
		Power on self-test failure if the led always stays solid red.
	Flash Red	Firmware upgrades in progress
ADSL	Off	No ADSL signal is detected.
	Slow Flash Green	ADSL line is handshaking in progress
	Fast Flash Green	ADSL line is training in progress
	Solid Green	ADSL line connection is up.
PPP	Off	No PPPoA or PPPoE connection
	Solid Green	At least one PPPoA or PPPoE connection is up. The users can access the Internet now.
Ethernet	Off	No Ethernet signal is detected.
	Flash Green	User data is going through Ethernet port
	Solid Green	Ethernet interface is ready to work.
USB	Off	No USB signal is detected.
	Flash Green	User data is going through USB port
	Solid Green	USB interface is ready to work.
WLAN	Off	No radio signal is detected or WLAN has been disabled.
	Flash Green	User data is going through WLAN port
	Solid Green	WLAN interface is ready to work.

NB6W Rear Panel

The following figure illustrates the rear panel of your ADSL Router:



Connector	Description
	Wireless antenna
Power	12VAC Power connector
	Power on/off switch
Reset	Reset to factory defaults
Ethernet	Ethernet RJ-45 connector
USB	USB connector
Line	RJ-11 connector (Telephone line)

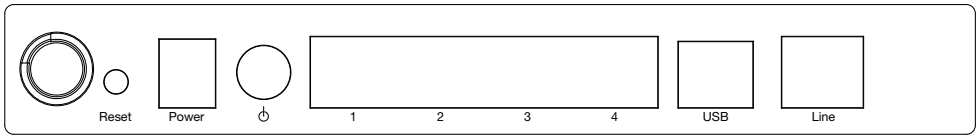
NB6Plus4W LED Indicators

The LED Indicators are located on the front of the unit, their meanings are as follows:

Function	Color	Definition
Power	Off	Power is off.
	Solid Green	Power is on and the device operates normally.
	Solid Red	Power on self-test in progress
		The device enters the console mode of the boot loader.
		Power on self-test failure if the led always stays solid red.
	Flash Red	Firmware upgrades in progress
ADSL	Off	No ADSL signal is detected.
	Slow Flash Green	ADSL line is handshaking in progress
	Fast Flash Green	ADSL line is training in progress
	Solid Green	ADSL line connection is up.
PPP	Off	No PPPoA or PPPoE connection
	Solid Green	At least one PPPoA or PPPoE connection is up. The users can access the Internet now.
Ethernet 1, 2, 3, 4	Off	No Ethernet signal is detected.
	Flash Green	User data is going through Ethernet port
	Solid Green	Ethernet interface is ready to work.
USB	Off	No USB signal is detected.
	Flash Green	User data is going through USB port
	Solid Green	USB interface is ready to work.
WLAN	Off	No radio signal is detected or WLAN has been disabled.
	Flash Green	User data is going through WLAN port
	Solid Green	WLAN interface is ready to work.

NB6Plus4W Rear Panel

The following figure illustrates the rear panel of your ADSL Router:



Connector	Description
	Wireless antenna
Reset	Reset to factory defaults
Power	12VAC Power connector
	Power on/off switch
Ethernet – 1, 2, 3, 4	Ethernet RJ-45 connector
USB	USB connector
Line	RJ-11 connector (Telephone line)

CHAPTER 2: SYSTEM REQUIREMENT AND INSTALLATION

System Requirements

Before continuing with the installation of your Modem Router please confirm that you comply with the minimum system requirements.

- Pentium® MMX 233MHz
- A CD-ROM Drive
- Ethernet card installed with TCP/IP Protocol
  (required when connecting to the ETHERNET port of your ADSL Router)
- OS independent for Ethernet
- USB Port (required only if you are connecting to the USB Port of your ADSL Router)
- Host Operating Systems support for USB:
  - Windows® 98 Second Edition
  - Windows® 2000
  - Windows® Me
  - Windows® XP (recommended)
- Web Browser support:
  - Microsoft Internet Explorer 5.0 (or later versions)
  - Netscape® Navigator 4.0 (or later versions)
  - Most popular browsers

To access the ADSL Router via Ethernet (Recommended), the host computer must meet the following requirements:

- Equipped with an Ethernet network interface.
- Have TCP/IP installed.
- Allow the client PC to obtain an IP address automatically or set a fixed IP address.
- With a web browser installed: Internet Explorer 5.x or later.

The ADSL Router is configured with the default IP address of 192.168.1.1 and subnet mask of 255.255.255.0. Considering that the DHCP server is Enable by default, the DHCP clients should be able to access the ADSL Router, or the host PC should be assigned an IP address first for initial configuration.

You also can manage the ADSL Router through a web browser-based manager: ADSL ROUTER CONTROL PANEL. The ADSL Router manager uses the HTTP protocol via a web browser to allow you to set up and manage the device.

To configure the device via web browser, at least one properly-configured PC must be connected to the network (either connected directly or through an external hub/switch to the LAN port of the device).

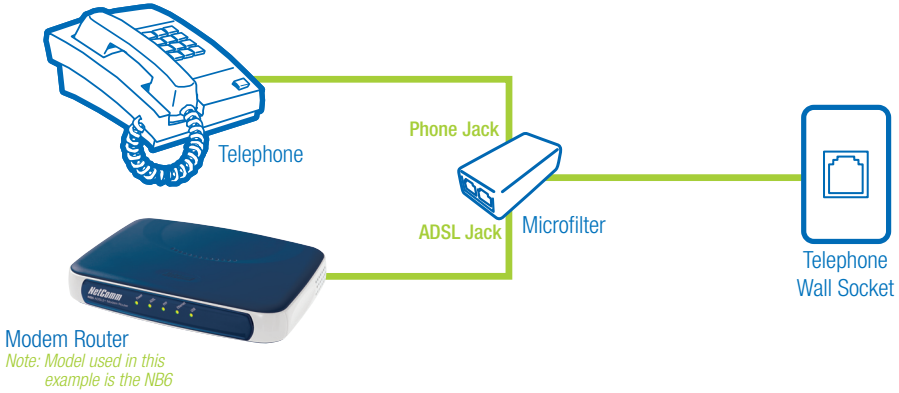
Do I need a Micro filter?

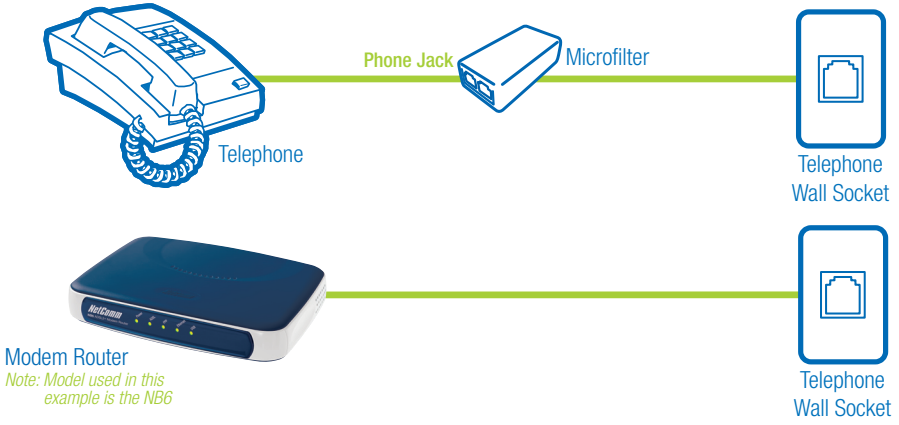
An ADSL Microfilter filters out ADSL signals to allow ADSL and regular Voice Calls to share a single telephone line.

Any equipment sharing your ADSL telephone line, other than an ADSL modem must be connected to a telephone jackpoint via a microfilter. Examples of such non-ADSL equipment that MUST connect through a microfilter are :

- Telephone Handset
- Fax Machine
- Foxtel digital set
- Back to base alarm
- Modem (non adsl)
- Caller display unit
- Other devices that have an integral modem

Failure to connect ALL non-ADSL equipment via a microfilter may result in loss of the data link whenever a call is made or answered. In many cases the link will also be lost when a call is received even if it is not answered.





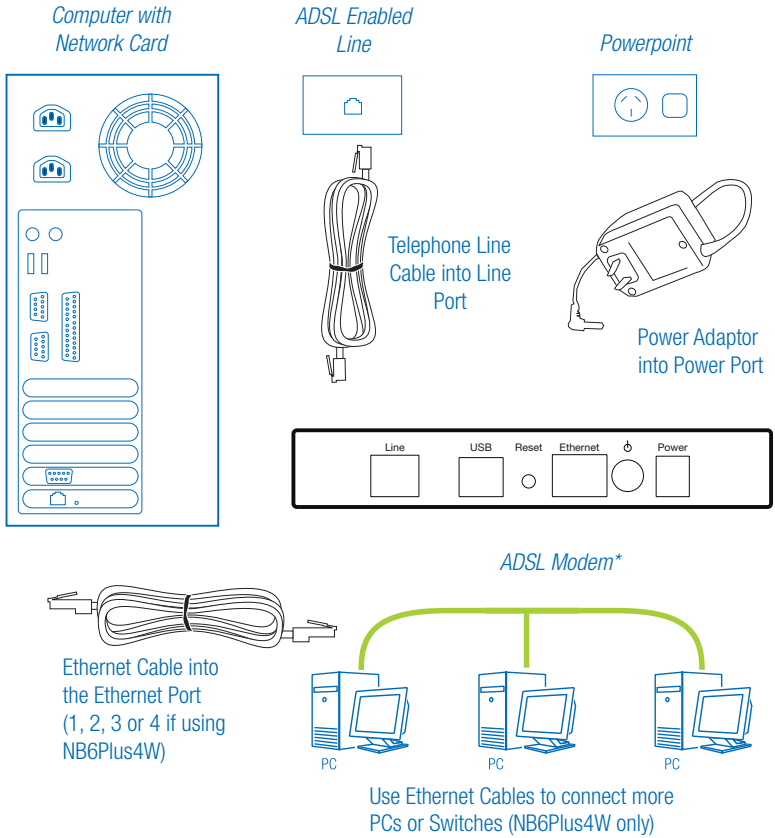
Choosing a place for the ADSL Router

- Place the ADSL Router close to ADSL wall outlet and power outlet for the cable to reach it easily.
- Avoid placing the device in places where people may walk on the cables. Also keep it away from direct sunlight or heat sources.
- Place the device on a flat and stable stand.

Connecting the ADSL Router (Ethernet)

Follow the steps below to connect the related devices.

- Connecting the ADSL line. Connect the DSL port of the device to your ADSL wall outlet with RJ-11 cable.
- Please attach one end of the Ethernet cable with RJ-45 connector to the LAN port of your ADSL Router.
- Connect the other end of the cable to the Ethernet port of the client PC.
- Connect the supplied power adapter to the Power port of your ADSL Router, and plug the other end to a power outlet.
- Turn on the power switch.



** Model shown is NB6, NB6W and NB6Plus4W vary slightly from image*

USB Driver Installation

If the ADSL router is to be connected to a PC through the USB interface, you will need to install the USB drivers prior to plugging the USB cable to the PC. Refer to the relevant operating system below to install the USB drivers.

Note: Do not connect the USB cable until you are prompted to in the instructions below

For Windows ME

- Run the USB installation program from the CD provided in your router package.
- An InstallShield Wizard will appear. Please wait for a moment.
- When the welcome screen appears, click Next for the next step.
- When the complete window of the InstallShield Wizard appears, click Finish.
- Link your router and the PC with a USB cable.
- The system will detect the USB driver automatically. Then, the system will copy the proper files for the router.

  Note: If the USB device is not detected automatically, check the USB cable between the PC and the device. Besides, verify that the device is power on.
- When the file copying finished, the dialog above will close. Now the USB driver is installed properly. You can use the router.

For Windows 2000

- Run the USB installation program from the CD provided in your router package.
- An InstallShield Wizard will appear. Please wait for a moment.
- When the welcome screen appears, click Next for the next step.
- When the complete window of the InstallShield Wizard appears, click Finish.
- Link your router and the PC with a USB cable.
- The system will detect the USB driver automatically, and then copy the proper files for the router.

  Note: If the USB device is not detected automatically, check the USB cable between the PC and the device. Besides, make sure that the device is power on.
- When the file copying is finished, the dialog above will close. Now the USB driver is installed properly. You can use the router.

To make sure that your router is properly installed, please do the following steps.

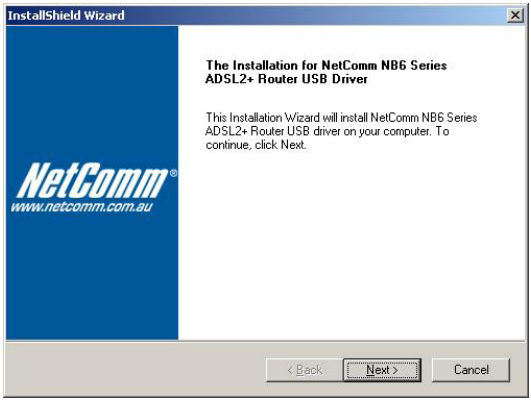
1. Right-click on My Computer and press Properties.
2. On the Hardware tab, click Device Manager.
3. Confirm that the NetComm NB6 Series ADSL Router USB Remote NDIS Device is on the Network adapters list.

For Windows XP

- Run the USB installation program from the CD provided in your router package.
- An InstallShield Wizard will appear. Please wait for a moment.

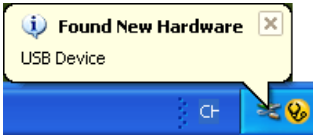
InstallShield Wizard
NetComm NB6 Series ADSL2+ Router USB Driver Setup is preparing the InstallShield® Wizard, which will guide you through the rest of the setup process. Please wait.
Cancel

- When the welcome screen appears, click Next for the next step.

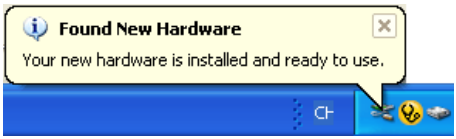

InstallShield Wizard
The Installation for NetComm NB6 Series ADSL2+ Router USB Driver
This Installation Wizard will install NetComm NB6 Series ADSL2+ Router USB driver on your computer. To continue, click Next.
NetComm
www.netcomm.com.au
< Back
Next >
Cancel

- When the finish installing message of InstallShield Wizard appears, click Finish.
- Link your router and the PC with a USB cable.
- The system will detect the USB driver automatically.

Note: If the USB device is not detected, check the USB cable between the PC and the device. Also make sure that the device is power on.



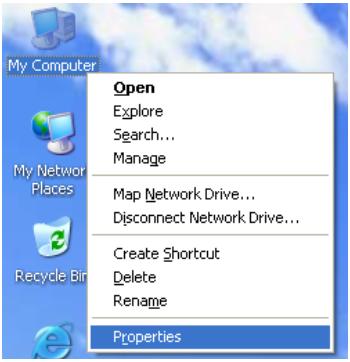
- The system will then try to find the proper driver for your router and copy the files automatically.
- After the file copying finished, a completing message will appear.



- You can use your router now.

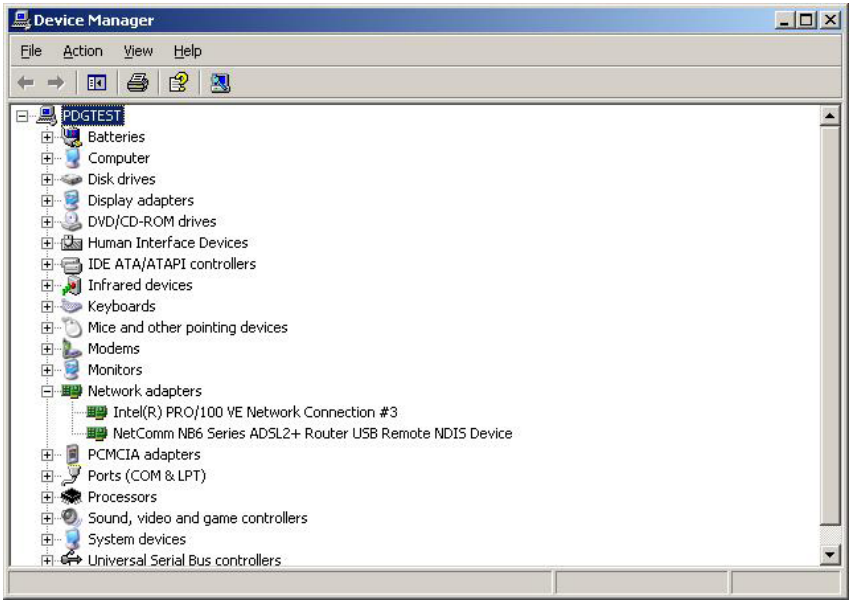
To make sure your router is properly installed, please do the following steps.

1. Right-click on My Computer and press Properties.



2. On the Hardware tab, click Device Manager.

3. Confirm that the NetComm NB6 ADSL Router USB Remote NDIS Device is on the Network adapters list.



Uninstalling the USB Driver

For Windows ME

To uninstall the USB driver, please follow the procedure below.

- Unplug the USB cable between your router and your PC. Then click OK.
- Choose Settings –Control Panel from the Start menu. Choose Add/Remove Programs.
- A dialog appears to ask you to choose the program that you want to remove. Please select NetComm ADSL Router USB Driver and click Change/Remove.
- The InstallShield Wizard dialog will appear.
- When the Maintenance Complete screen appears, the USB driver is removed successfully. Click Finish

For Windows 2000

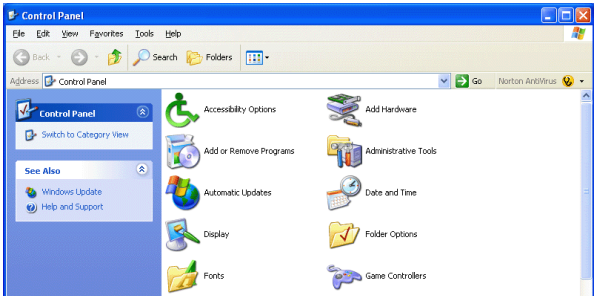
To uninstall the USB driver, please follow the procedure below.

- To safely unplug the USB cable from the USB port on your PC:
  1. Go to the right lower corner for Unplug and Eject Hardware and left click on it.
  2. Click the dialog for Stop NetComm ADSL Router USB Remote NDIS Device.
  3. The Router is safely removed, click OK to continue.
- Choose Settings – Control Panel from the Start menu. Choose Add/Remove Programs.
- A dialog appears to ask you to choose the program that you want to remove. Please select NetComm ADSL Router USB Driver and click Change/Remove.
- A Confirm Uninstall dialog will show up, unplug your device from the USB port and click OK.
- The InstallShield Wizard will guide you till the USB driver is removed.
- When the Maintenance Complete screen appears, the USB driver is removed successfully. Click Finish.

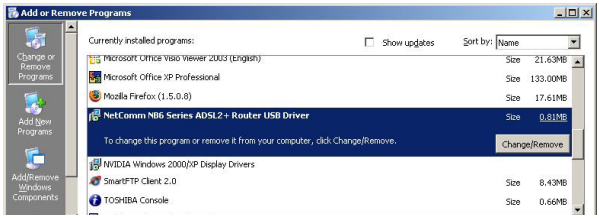
For Windows XP

To uninstall the USB driver, please follow the procedure below.

- Unplug your USB cable between your router and your PC.
- Choose Settings –Control Panel from the Start menu. Choose Add or Remove Programs.



- A dialog appears to ask you to choose the program that you want to remove. Please select NetComm ADSL Router USB Driver and click Change/Remove.


Add or Remove Programs
Change or Remove Programs
Add New Programs
Add/Remove Windows Components
Currently installed programs:
Show updates
Sort by: Name
Microsoft Office Visio Viewer 2003 (English) Size 21.63MB
Microsoft Office XP Professional Size 133.00MB
Mozilla Firefox (1.5.0.8) Size 17.61MB
NetComm NB6 Series ADSL2+ Router USB Driver Size 0.81MB
To change this program or remove it from your computer, click Change/Remove.
Change/Remove
NVIDIA Windows 2000/XP Display Drivers
SmartFTP Client 2.0 Size 8.43MB
TOSHIBA Console Size 0.66MB

- The InstallShield Wizard dialog will appear.

InstallShield Wizard
NetComm NB6 Series ADSL2+ Router USB Driver Setup is preparing the InstallShield® Wizard, which will guide you through the rest of the setup process. Please wait.
Cancel

- A dialog appears to confirm whether you want to remove the USB driver or not. Unplug the USB cable from your PC, and click Ok.

Confirm Uninstall
Do you want to remove the NetComm NB6 Series ADSL2+ Router USB driver?
Warning: Please unplug the USB cable now before proceeding with uninstall.
OK
Cancel

- When the Maintenance Complete screen appears, the USB driver is removed successfully. Click Finish.

Setting up TCP/IP

In order to access the Internet through the ADSL Router, each host on your network must install/setup TCP/IP first. Please follow the steps below to set your network adapter.

If the TCP/IP protocol has not been installed yet, please follow the steps below for installation. In the following illustrations, we will set the PC to **get an IP address automatically at the same time**.

For Windows 98

1. Open the Start menu, point to Settings and click on Control Panel.
2. Double-click the Network icon.
3. The Network window appears. On the Configuration tab, check out the list of installed network components.
   Option 1: If there is no TCP/IP protocol, click Add.
   Option 2: If you have TCP/IP protocol, skip to Step 6.
4. Highlight Protocol and click Add.
5. Highlight Microsoft on the left side of the window, and select TCP/IP on the right side. Then click OK.
6. When returning to the Network window, highlight TCP/IP protocol for your NIC and click Properties.
7. On the IP Address tab: Enable Obtain an IP address automatically and click OK.
8. When returning to the Network window, click OK
9. Wait for Windows when copying files.
10. When prompted with System Settings Change dialog box, click Yes to restart your computer.

For Windows ME

1. Open the Start menu, point to Settings and click on Control Panel.
2. Double-click the Network icon.
3. The Network window appears. On the Configuration tab, check out the list of installed network components.
   Option 1: If there is no TCP/IP protocol, click Add.
   Option 2: If you have TCP/IP protocol, skip to Step 6.
4. Highlight Protocol and click Add.
5. Highlight Microsoft on the left side of the windows, and select TCP/IP on the right side. Then click OK.
6. While returning to Network window, highlight TCP/IP protocol for your NIC and click Properties.
7. On IP Address tab: Enable Obtain an IP address automatically and click OK.
8. While returning to the Network window, click OK.
9. Wait for Windows when copying files.
10. When prompted with the System Settings Change dialog box, click Yes to restart your computer.

For Windows NT

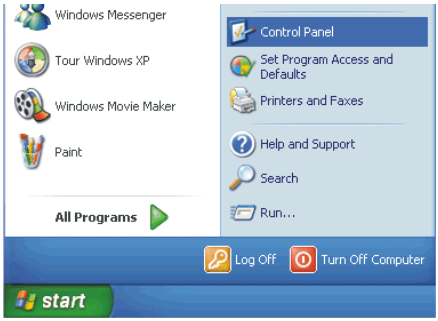
1. Click Start, point to Settings, and then click Control Panel.
2. Double-click the Network icon.
3. The Network window appears. On the Protocols tab, check out the list of installed network components.
   Option 1: If there is no TCP/IP Protocol, click Add.
   Option 2: If you have TCP/IP Protocol installed, skip to Step 7.
4. Highlight TCP/IP Protocol and click OK.
5. Insert the Windows NT CD into your CD-ROM drive and type the location of the CD. Then click Continue.
6. When returning to the Network window. Open the Protocols tab, then select TCP/IP Protocol and click Properties.
7. Enable Obtain an IP address from a DHCP server and click OK.
8. When prompted with the message below, click Yes to continue.
9. When returning to Network window, click Close.
10. When prompted with Network Settings Change dialog box, click Yes to restart your computer.

For Windows 2000

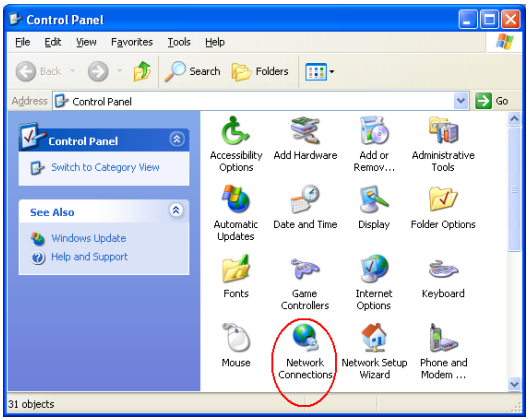
1. From the Start menu, point to Settings and then click Network and Dial-up Connections.
2. Right-click the Local Area Connection icon and then click Properties.
3. On the General tab, check out the list of installed network components.
   Option 1: If there is no TCP/IP Protocol, click Install.
   Option 2: If you have TCP/IP Protocol, skip to Step 6.
4. Highlight Protocol and then click Add.
5. Click Internet Protocol (TCP/IP) and then click OK.
6. When returning to the Local Area Connection Properties window, highlight Internet Protocol (TCP/IP) and then click Properties.
7. Under the General tab, enable Obtain an IP address automatically. Then click OK.

For Windows XP

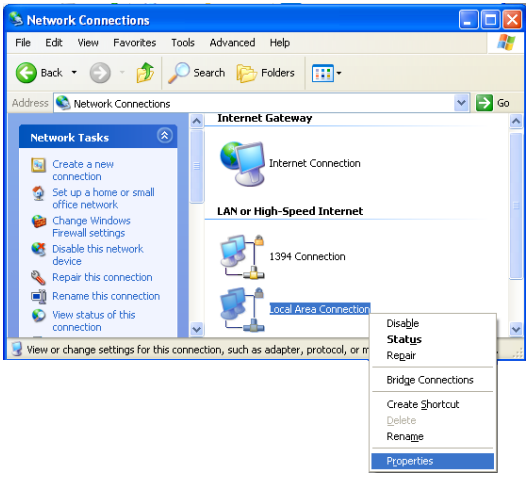
1. Open the Start menu, point to Control Panel and click it.



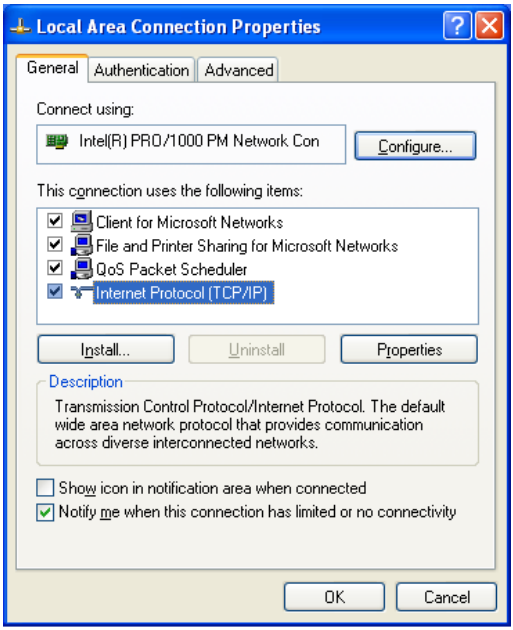
2. Double click the Network Connection.



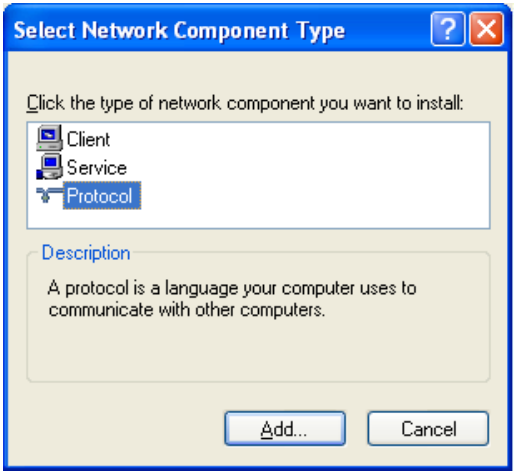
3. Right click Local Area Connection and then click Properties.



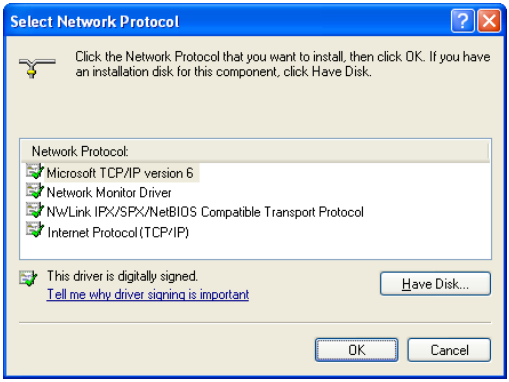
4. On the General tab, check out the list of installed network components.
   Option 1: If there is no TCP/IP Protocol, click Install.
   Option 2: If you have TCP/IP Protocol, skip to Step 7.



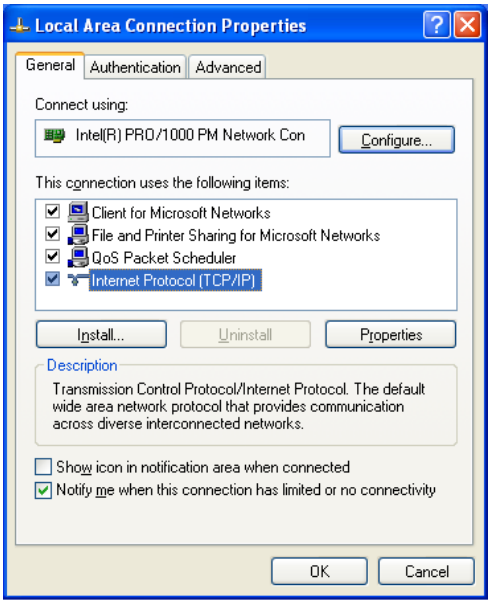
5. Highlight Protocol and then click Add.



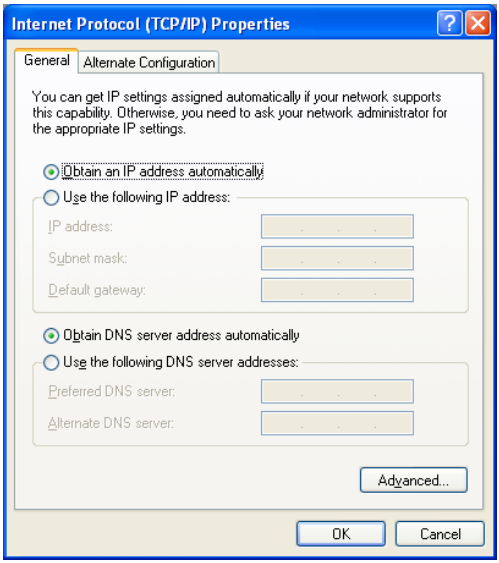
6. Click Internet Protocol(TCP/IP) and then click OK.


Select Network Protocol
Click the Network Protocol that you want to install, then click OK. If you have an installation disk for this component, click Have Disk.
Network Protocol:
Microsoft TCP/IP version 6
Network Monitor Driver
NWLink IPX/SPX/NetBIOS Compatible Transport Protocol
Internet Protocol (TCP/IP)
This driver is digitally signed.
Tell me why driver signing is important
Have Disk...
OK
Cancel

7. When it returns to the General Tab on the Local Area Connection Properties window, highlight Internet Protocol (TCP/IP) and then click Properties.



8. Under the General tab, select Obtain an IP address automatically, and Obtain DNS server address automatically. Then click Ok.

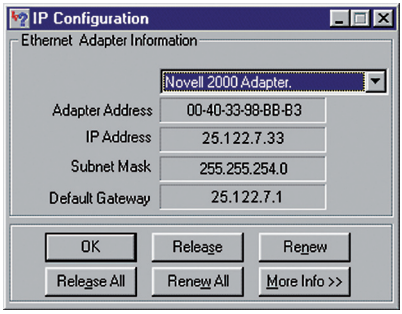

Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Renewing IP Address on Client PC

After the ADSL Router gets on line, there is a chance that your PC does not renew its IP address and thus causes the PC not able to access the Internet. To solve this problem, please follow the procedures below to renew PC's IP address.

For Windows 98/ME

1. Select Run from the Start menu.
2. Type winipcfg in the text box and click OK.
3. When the figure below appears, click Release to let go of the address and then click the Renew button to obtain a new IP address.



For Windows NT/2000/XP

1. Open the Start menu, and click Run... on this menu.
2. Type cmd in the text box that appears and click OK. Then you will see the command prompt window.
   - Another way to open the command prompt:
   - From Start menu, point to Programs, select Accessories, and then click Command Prompt.
3. Type ipconfig at the command prompt window and press Enter to view the computer's IP information from DHCP server.
4. If the computer is holding a current IP address, type ipconfig /release to let go of the address, then type ipconfig /renew to obtain a new one.

CHAPTER 3: ACCESSING THE INTERNET

This chapter aims to help you access the Internet in a quick and convenient way. If you need more detailed information for web configuration, please refer to the next chapter for the advanced configuration.

Before configuring the ADSL Router, you must decide whether to configure the ADSL Router as a bridge or as a router. This chapter presents some deployment examples for your reference. Each mode includes its general configure procedures. For more detailed information about web configuration, refer to “Web Configuration”.

- PPP over ATM (PPPoA)
- PPPoA IP Extenstion
- PPP over Ethernet (PPPoE)
- PPPoE IP Extension
- Numbered IP over ATM (IPoA)
- Numbered IP over ATM (IPoA) + NAT
- Unnumbered IP over ATM (IPoA)
- Unnumbered IP over ATM (IPoA) + NAT
- Bridge Mode
- MER (Bridge Mode + NAT)

To ensure your PC accessing the Internet successfully, please check the following first.

- A network interface card is installed on your PC.
- The ADSL Router is solidly connected with your computer.
- The TCP/IP protocol has been installed and the IP address setting is to obtain IP address automatically.

When all above preparations are ready, you can open the Browser and type “192.168.1.1” into the URL box and start to make the web configuration for different connection modes.

This chapter is going to introduce the function of each connection mode and the basic configuring steps that you have to do. If you do not follow the configuring steps for using these connection modes, you might get some connection problems and cannot connect to the Internet well.

PPP over ATM (PPPoA) Mode

Description:

In this deployment environment, the PPPoA session is between the ADSL WAN interface and BRAS. The ADSL Router gets a public IP address from BRAS when connecting to DSLAM. The multiple client PCs will get private IP address from the DHCP server enabled on private LAN. The enabled NAT mechanism will translate the IP information for clients to access the Internet.

Configuration:

1. Start your browser and type **192.168.1.1** as the address to access ADSL web-based manager.
2. Go to **Quick Start** – **Quick Setup**. Uncheck **Auto Scan Internet Connection (PVC)**. Key in the **VCI** and **VPI** value, e.g.:
   - **VPI** – 8
   - **VCI** – 35

   Click the **Next** button.
3. On the **Configure Internet Connection** – **Connection Type** page, select **PPP over ATM (PPPoA)** then click the **Next** button.
4. On the **WAN IP Settings** page, select **Obtain an IP address automatically** and check **Enable NAT box**. Click **Next**.
5. On the **PPP Username and Password** page, enter the PPP username and password that you got from your ISP. Select **Always on** or select **Dial on Demand** and key in the inactivity timeout value. (The default value is 20 minutes.) Then click **Next**.
6. On the **Configure LAN side Settings** page, key in the IP address and subnet mask for your LAN, e.g.:
   Primary IP address: 192.168.1.1

   Subnet Mask: 255.255.255.0

   Check **DHCP Server on** box. And key in the start and end IP address, e.g.:
   Start IP Address:192.168.1.2

   End IP Address: 192.168.1.254

   Then enter the leased time (the default is 1 day), and click **Next**.
7. Check the network information on **This Internet Connection** -- **Summary** page. Make sure the settings match the information provided by your ISP. Click **Finish**.

PPP over ATM (PPPoA) IP Extension Mode

Description:

In this deployment environment, the PPPoA session is between the ADSL WAN interface and BRAS. The ADSL Router acts as a bridge and receives a public IP address from BRAS for your computer. And only the one that bears the public IP address is allowed to access the Internet. Moreover, no NAT translation will be done at this case.

Configuration:

1. Start your browser and type **192.168.1.1** in the URL box to access ADSL web-based manager.
2. Go to **Advanced** – **Internet** – **Connections**. And click **Add**.
3. Key in the **VCI** and **VPI** value, e.g.:
   - **VPI** – 8
   - **VCI** – 35

   Click the **Next** button.
4. On the **Configure Internet Connection** – **Connection Type** page, select **PPP over ATM (PPPoA)** then click the **Next** button.
5. On the **WAN IP Settings** page, select **Obtain an IP address automatically**, check **PPP IP extension** (and **Enable NAT** would become disabled automatically) then click **Next**.
6. On the **PPP Username and Password** page, enter the PPP username and password offered by your ISP. Select **Always on**, and then click **Next**.
7. Check the network information on **This Internet Connection** -- **Summary** page. Make sure the settings match the settings provided by the ISP. Click **Apply**.
8. Press **Finish**.

PPP over Ethernet (PPPoE) Mode

Description:

In this deployment environment, the PPPoE session is between the ADSL WAN interface and BRAS. The ADSL Router gets a public IP address from BRAS when connecting to DSLAM. The multiple client PCs will get private IP address from the DHCP server enabled on private LAN. The enabled NAT mechanism will translate the IP information for clients to access the Internet.

Configuration:

1. Start your browser and type **192.168.1.1** in the URL box to access ADSL web-based manager.
2. Go to **Quick Start** – **Quick Setup**. Uncheck **Auto Scan Internet Connection (PVC)**. Key in the **VCI** and **VPI** value, e.g.:
   - **VPI** – 8
   - **VCI** – 35

   Click the **Next** button.
3. On the **Configure Internet Connection** – **Connection Type** page, select **PPP over Ethernet (PPPoE)** then click the **Next** button.
4. On the **WAN IP Settings** page, select **Obtain an IP address automatically** and check **Enable NAT** box. Click Next.
5. On the **PPP Username and Password** page, enter the PPP username and password that you got from your ISP. Select **Always on** or select **Dial on Demand** and key in the inactivity timeout value. (The default value is 20 minutes.) Then click **Next**.
6. On the **Configure LAN side Settings** page, key in the IP address and subnet mask for your LAN, e.g.:
   Primary IP address: 192.168.1.1

   Subnet Mask: 255.255.255.0

   Check DHCP Server on box. And key in the start and end IP address, e.g.:
   Start IP Address:192.168.1.2

   End IP Address: 192.168.1.254

   Then enter the leased time (the default is 1 day), and click **Next**.
7. Check the network information on **This Internet Connection** -- **Summary** page. Make sure the settings match the information provided by your ISP. Click **Finish**.

PPP over Ethernet (PPPoE) IP Extension Mode

Description:

In this deployment environment, the PPPoE session is between the ADSL WAN interface and BRAS. The ADSL Router acts as a bridge and gets a public IP address from BRAS for your computer. And only the one that got the public IP address is allowed to access into Internet. The real IP that you got is acquired from ISP. Moreover, no NAT translation will be done at this case.

Configuration:

1. Start your browser and type **192.168.1.1** in the URL box to access ADSL web-based manager.
2. Go to **Advanced** – **Internet** – **Connections**. And click **Add**.
3. Key in the **VCI** and **VPI** value, e.g.:
   - **VPI** – 8
   - **VCI** – 35

   Click the **Next** button.
4. On the **Configure Internet Connection** – **Connection Type** page, select **PPP over Ethernet (PPPoE)** then click the **Next** button.
5. On the **WAN IP Settings** page, select **Obtain an IP address automatically**, check **PPP IP extension** (and **Enable NAT** would become disabled automatically) then click **Next**.
6. On the **PPP Username and Password** page, enter the PPP username and password offered by your ISP. Select **Always on**, and then click **Next**.
7. Check the network information on **This Internet Connection** -- **Summary** page. Make sure the settings match the settings provided by the ISP. Click **Apply**.
8. Press **Finish**.

Numbered IP over ATM (IPoA)

Description:

If you apply for multiple IP addresses from your ISP, you can assign these public IP addresses to the ADSL Router and public server, e.g., Web or FTP server. Typically the first IP is network address, the second is used as router IP address and the last one is for subnet broadcasting. Other remaining IP addresses can be assigned to PCs on the LAN. The following example uses the LAN IP address ranging from 10.11.80.81 to 10.11.80.86 and the subnet mask for LAN is 255.255.255.248. The WAN IP address is 10.11.95.233, and the subnet mask for WAN is 255.255.255.248.

Configuration:

1. Start your browser and type **192.168.1.1** in the URL box to access ADSL web-based manager.
2. Go to **Quick Start** – **Quick Setup**. Uncheck **Auto Scan Internet Connection (PVC)**. Key in the **VCI** and **VPI** value, e.g.:
   - **VPI** – 8
   - **VCI** – 35

   Click the **Next** button.
3. On the **Configure Internet Connection** – **Connection Type** page, select **IP over ATM (IPoA)** then click **Next**.
4. On the **WAN IP Settings** page, select **Use the following IP address** and **Use the following DNS Server Address**, then key in the information that your ISP offered, e.g.:

   WAN IP Address: 10.11.95.233

   WAN Subnet Mask: 255.255.255.248

   Primary DNS server: 168.95.1.1

   Secondary DNS server: 168.95.192.1

   Uncheck **Enable NAT** and click **Next**.
5. On the **Configure LAN side Settings** page, key in the information for your LAN, e.g.,

   Primary IP Address: 192.168.1.1

   Subnet mask: 255.255.255.0

   Start IP Address: 192.168.1.2

   End IP Address: 192.168.1.254
6. Check **Configure the second IP Address and Subnet Mask for LAN Interface** and enter the information needed.

   Secondary IP Address: 10.11.80.81

   Subnet mask: 255.255.255.248

   Click **Next**.
7. Check the network information on the **Summary** page. Make sure the settings match the settings provided by your ISP. Click **Finish**.
8. Refer to the TCP/IP properties, specify an IP Address, and fill in other information needed, e.g.:

   IP Address: 10.11.80.82

   Subnet Mask: 255.255.255.248

   Gateway: 10.11.80.81

   Preferred DNS server: 168.95.1.1
9. Now the router is correctly configured. You can access the Internet.

Numbered IP over ATM (IPoA)+NAT

Description:

In this deployment environment, we make up a private IP network of 192.168.1.1. NAT function is enabled (on ADSL Router or use another NAT box connected to hub) to support multiple clients to access the Router and some public servers (WWW, FTP).

If you apply for multiple IP addresses from your ISP, you can assign these public IP addresses to the ADSL Router and public server, e.g., Web or FTP server. Typically the first IP is network address, the second is used as router IP address and the last one is subnet broadcasting. Other remaining IP addresses can be assigned to PCs on the LAN.

The following example uses the IP address ranging from 10.11.80.81 to 10.11.80.86 and the subnet mask is 255.255.255.248.

Configuration:

1. Start your browser and type **192.168.1.1** in the URL box to access ADSL web-based manager.
2. Go to **Quick Start** – **Quick Setup**. Uncheck **Auto Scan Internet Connection (PVC)**. Key in the **VCI** and **VPI** value, e.g.:
   - **VPI** – 8
   - **VCI** – 35

   Click the **Next** button.
3. On the **Configure Internet Connection** – **Connection Type** page, select **IP over ATM (IPoA)** then click **Next**.
4. On the **WAN IP Settings** page, select **Use the following IP address** and **Use the following DNS Server Address**, then key in the information that your ISP offered, e.g.:

   WAN IP Address: 10.11.80.81

   WAN Subnet Mask: 255.255.255.248

   Primary DNS server: 168.95.1.1

   Secondary DNS server: 168.95.192.1
5. Check the **Enable NAT** box. And click **Next**.
6. On the **Configure LAN side Settings** page, key in the information for your LAN, e.g.,

   Primary IP Address: 192.168.1.1

   Subnet mask: 255.255.255.0

   Start IP Address: 192.168.1.2

   End IP Address: 192.168.1.254
7. Check the network information. Make sure the settings match the settings provided by ISP. Click **Finish**.
8. Now the router is correctly configured. You can access into Internet.

Unnumbered IP over ATM (IPoA)

Description:

If you apply for multiple IP addresses from your ISP, you can assign these public IP addresses to the ADSL Router and public server, e.g., Web or FTP server. Typically the first IP is network address, the second is used as router IP address and the last one is subnet broadcasting. Other remaining IP addresses can be assigned to PCs on the LAN.

The following example uses the IP address ranging from 10.11.80.81 to 10.11.80.86 and the subnet mask is 255.255.255.248. In such circumstance, we do not assign any WAN IP.

Configuration:

1. Start your browser and type **192.168.1.1** in the URL box to access ADSL web-based manager.
2. Go to **Quick Start** – **Quick Setup**. Uncheck **Auto Scan Internet Connection (PVC)**. Key in the **VCI** and **VPI** value, e.g.:
   - **VPI** – 8
   - **VCI** – 35

   Click the **Next** button.
3. On the **Configure Internet Connection** – **Connection Type** page, select **IP over ATM (IPoA)** then click **Next**.
4. On the **WAN IP Settings** page, select **None** for WAN IP address settings. Then, select **Use the following DNS Server Address** and key in the information that your ISP offered, e.g.:

   Primary DNS server: 168.95.1.1

   Secondary DNS server: 168.95.192.1

   Uncheck **Enable NAT** and click **Next**.
5. On the **Configure LAN side Settings** page, key in the information for your LAN, e.g.,

   Primary IP Address: 192.168.1.1

   Subnet mask: 255.255.255.0

   Start IP Address: 192.168.1.2

   End IP Address: 192.168.1.254
6. Check **Configure the second IP Address** and **Subnet Mask** for LAN Interface and enter the information needed, e.g.,

   Secondary IP Address: 10.11.80.81

   Subnet mask: 255.255.255.248

   Check **DHCP Server Off** and click **Next**.
7. Check the network information on the **Summary** page. Make sure the settings match the settings provided by your ISP. Click **Finish**.
8. Refer to the TCP/IP properties, specify an IP Address, and fill in other information needed, e.g.:

   IP Address: 10.11.80.82

   Subnet Mask: 255.255.255.248

   Gateway: 10.11.80.81

   Preferred DNS server: 168.95.1.1
9. Now the router is correctly configured. You can access the Internet.

Unnumbered IP over ATM (IPoA)+NAT

Description:

If you apply for multiple IP addresses from your ISP, you can assign these public IP addresses to the ADSL Router and public server, e.g., Web or FTP server. Typically the first IP is network address, the second is used as router IP address and the last one is subnet broadcasting. Other remaining IP addresses can be assigned to PCs on the LAN.

The following example uses the IP address ranging from 10.11.80.81 to 10.11.80.86 and the subnet mask is 255.255.255.248. In such circumstance, we enable NAT function but not assign any WAN IP.

Configuration:

1. Start your browser and type **192.168.1.1** in the URL box to access ADSL web-based manager.
2. Go to **Quick Start** – **Quick Setup**. Uncheck **Auto Scan Internet Connection (PVC)**. Key in the **VCI** and **VPI** value, e.g.:
   - **VPI** – 8
   - **VCI** – 35

   Click the **Next** button.
3. On the **Configure Internet Connection** – **Connection Type** page, select **IP over ATM (IPoA)** then click **Next**.
4. On the **WAN IP Settings** page, select **None** for WAN IP address settings. Then, select **Use the following DNS Server Address** and key in the information that your ISP offered, e.g.:
   Primary DNS server: 168.95.1.1

   Secondary DNS server: 168.95.192.1
5. Check the **Enable NAT** box. And click **Next**.
6. On the **Configure LAN side Settings** page, key in the information for your LAN, e.g.,
   Primary IP Address: 192.168.1.1

   Subnet mask: 255.255.255.0

   Start IP Address: 192.168.1.2

   End IP Address: 192.168.1.254
7. Check **Configure the second IP Address** and **Subnet Mask** for LAN Interface and enter the information needed, e.g.,
   Secondary IP Address: 10.11.80.81

   Subnet mask: 255.255.255.248

   Click **Next**.
8. Check the network information on the **Summary** page. Make sure the contents match the settings provided by your ISP. Click Finish.
9. Now the router is correctly configured. You can access the Internet.

Bridge Mode

Description:

In this example, the ADSL Router acts as a bridge which bridging the PC IP addresses from LAN to WAN. The PC IP address can be a static public address that is pre-assigned by the ISP or a dynamic public address that is assigned by the ISP DHCP server, or an IP address received from PPPoE software.

Therefore, it does not require a public IP address. It only has a default private IP address (192.168.1.1) for management purpose.

Configuration:

1. Choose a client PC and set the IP as 192.168.1.x (x is between 2 and 254) and the gateway as 192.168.1.1.
2. Start your browser and type **192.168.1.1** in the URL box to access ADSL web-based manager.
3. Go to **Quick Start** – **Quick Setup**. Uncheck **Auto Scan Internet Connection (PVC)**. Key in the **VCI** and **VPI** value, e.g.,
   - **VPI** – 8
   - **VCI** – 35

   Then click the **Next** button.
4. On the **Configure Internet Connection** – **Connection Type** page, select **Bridging** then click the **Next** button.
5. On the **WAN IP Settings** page, select **None** for WAN IP address settings.
6. On the **Configure LAN side Settings** page, enter the IP address and subnet mask for your LAN, e.g.:
   Primary IP address: 192.168.1.1

   Subnet Mask: 255.255.255.0

   Choose **DHCP Server Off** and click **Next**.
7. Check the network information on the **Summary** page. Make sure the contents match the settings provided by your ISP. Click **Finish**.
8. Refer to the TCP/IP properties, specify an IP Address, and fill in other information needed, e.g.:
   IP Address: 10.11.86.81

   Subnet Mask: 255.255.255.248

   Gateway: 10.11.86.1

   Preferred DNS server: 168.95.1.1
9. Click **OK**. Now the router is correctly configured. You can access to the Internet.

MER

Description:

In this deployment environment, we make up a private IP network of 192.168.1.1. NAT function is enabled to support multiple clients to access to Internet.

In this example, the ADSL Router acts as a NAT device which translates a private IP address into a public address. Therefore multiple users can share with one public IP address to access the Internet through this router. The public address can be a static public address that is pre-assigned by ISP or a dynamic public address that is assigned by the ISP DHCP server.

Configuration:

1. Start your browser and type **192.168.1.1** in the URL box to access ADSL web-based manager.
2. Go to **Quick Start** – **Quick Setup**. Uncheck **Auto Scan Internet Connection (PVC)**. Key in the **VCI** and **VPI** value, e.g.,
   - **VPI** – 8
   - **VCI** – 35

   Then click the **Next** button.
3. On the **Configure Internet Connection** – **Connection Type** page, select **Bridging** and then click the **Next** button.
4. On the **WAN IP Settings** page, select **Obtain an IP address automatically**; then, select **Obtain DNS server address automatically**.
5. Check **Enable NAT**. Then click **Next**.
6. On the **Configure LAN side Settings** page, key in the IP address and subnet mask for your LAN. Check **DHCP Server On** box, and enter the start and end points, e.g.:

   Primary IP address:192.168.1.1

   Subnet Mask:255.255.255.0

   Start IP Address:192.168.1.2

   End IP Address: 192.168.1.254

   Then key in the leased time that you want. And click **Next**
7. Check the network information on the **Summary** page. Make sure the contents match the settings provided by your ISP. Click **Finish**.
8. Now the router is correctly configured. You can access the Internet.

CHAPTER 4: WEB CONFIGURATION

Some users might want to set specific configuration for the router such as firewall, data transmission rate…, and so on. This chapter will provide you advanced information of the web pages for the router for your reference.

Using Web-Based Manager

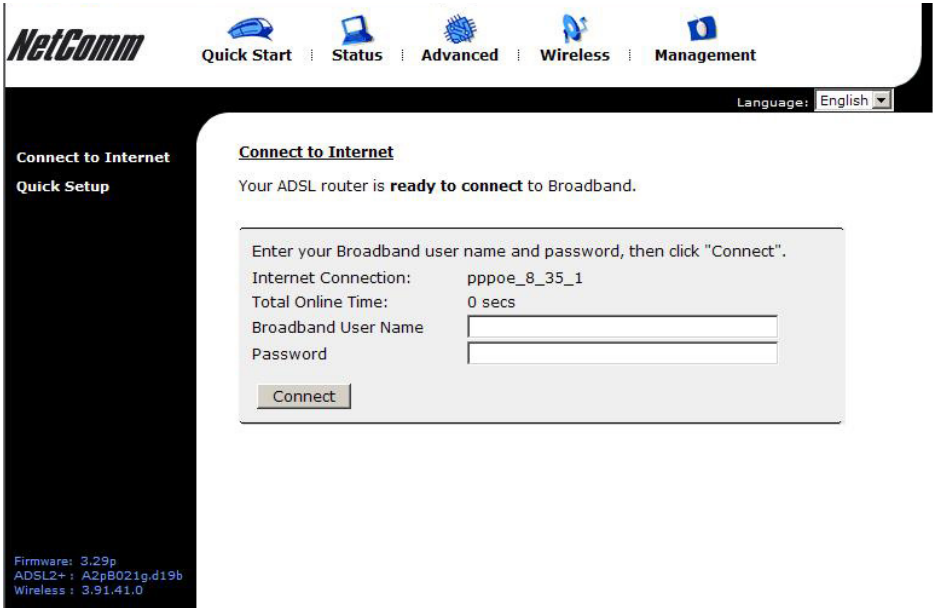
After properly configuring your host PC, please proceed as follows:

1. Start your web browser and type 192.168.1.1, the private IP address of the ADSL Router, in the URL field.
2. After connecting to the device, you will be prompted to enter username and password. By default, both the username and the password are **admin**. An example under Windows XP is shown below.

If you login successfully, the main page will appear. From now on, the ADSL Router acts as a web server sending HTML pages/forms on your request. You can fill in these pages/forms and apply them to the ADSL Router.

Outline of Web Manager

To configure the web page, please use admin as the username and the password. The main screen will be shown as below.



Title: The title of this management interface.

Main Menu: Including Quick Start, Status, Advanced, Wireless, and Management.

Main Window: The current workspace of the web manager, containing configuration or status information.

Current Version: Here provides the version info for firmware, ADSL2+, and Wireless.

To Have the New Settings Take Effect

After selecting or adjusting the settings according to your needs, your customizations will be saved to the flash memory before you restart the router. And only after rebooting the router, your customizations may take effect.

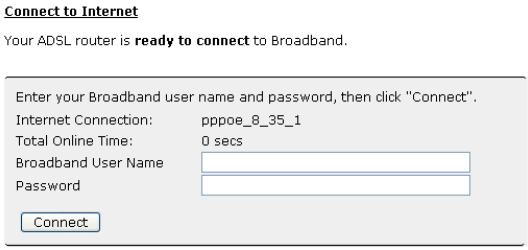
Language

On the top to the right of this web page, it provides a drop-down menu for you to choose a proper language. (However, we only offer English at present.)

Quick Start

The pages under the Quick Start menu provide user a quick way to set up the router. If you do not know much about the router, you can use the Quick Start pages to adjust basic settings to activate your router.

Connect to Internet

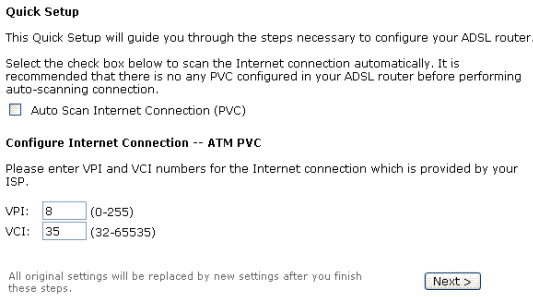


This is a quick way to connect to the Internet by using PPPoE interface, please click **Connect to Internet** to open the web page.

Enter the user name and password (that you get from the ISP) for your ADSL router and click **Connect**.

The system will connect automatically, and then you can access the Internet.

Quick Setup


Quick Setup
This Quick Setup will guide you through the steps necessary to configure your ADSL router.
Select the check box below to scan the Internet connection automatically. It is recommended that there is no any PVC configured in your ADSL router before performing auto-scanning connection.
Auto Scan Internet Connection (PVC)
Configure Internet Connection -- ATM PVC
Please enter VPI and VCI numbers for the Internet connection which is provided by your ISP.
VPI: 8 (0-255)
VCI: 35 (32-65535)
All original settings will be replaced by new settings after you finish these steps.
Next >

The quick setup wizard will guide you to configure the ADSL router through some specific steps. Yet different connection interface will lead to different setting pages. Refer to the following pages for detailed information.

Auto Scan Internet Connection (PVC):

If there is no any PVC configured in your ADSL router, you can check this item. Otherwise, please uncheck this box.

VPI (Virtual Path Identifier):

Identifies the virtual path between endpoints in an ATM network. The valid range is from 0 to 255. To enter the setting, please refer to the setting that the ISP offered.

VCI (Virtual Channel Identifier):

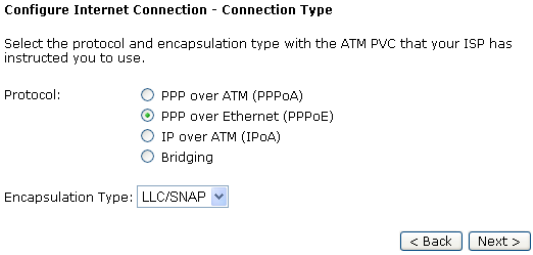
Identifies the virtual channel endpoints in an ATM network. The valid range is from 32 to 65535 (1 to 31 is reserved for well-known protocols). To enter the setting, please refer to the setting that the ISP gave you.

After entering the VPI/VCI value, please click **Next** for the following step.

Connection Type

The system provides several protocols for you to choose. Your ISP will offer you the most suitable settings of the protocol. Before you set this page, please refer to the protocol that your ISP offered.

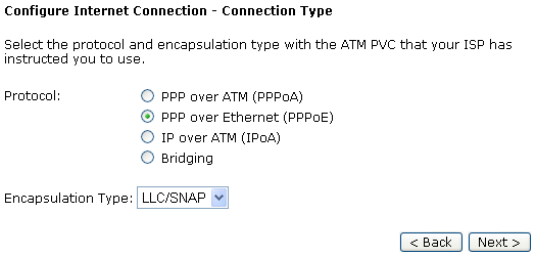
After clicking on the **Next** button from the VPI/VCI web page, the following screen will appear. Please choose the connection type and encapsulation mode that you want to use and click **Next** for next page.


Configure Internet Connection - Connection Type
Select the protocol and encapsulation type with the ATM PVC that your ISP has instructed you to use.
Protocol:
PPP over ATM (PPPoA)
PPP over Ethernet (PPPoE)
IP over ATM (IPoA)
Bridging
Encapsulation Type:
LLC/SNAP
< Back
Next >

For instance, PPP over Ethernet (PPPoE) is selected in this demonstrative figure.

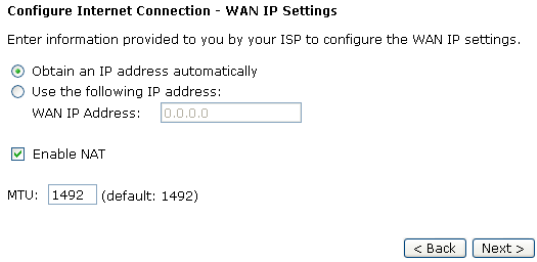
PPP over ATM/ PPP over Ethernet

If the connection type you choose is PPP over ATM or PPP over Ethernet, please refer to the following information.


Configure Internet Connection - Connection Type
Select the protocol and encapsulation type with the ATM PVC that your ISP has instructed you to use.
Protocol:
PPP over ATM (PPPoA)
PPP over Ethernet (PPPoE)
IP over ATM (IPoA)
Bridging
Encapsulation Type:
LLC/SNAP
< Back
Next >

According to the ISP's configuration on the server, you can choose PPPoE or PPPoA modes.

Choose **PPPoA** or **PPPoE** and click **Next**.


Configure Internet Connection - WAN IP Settings
Enter information provided to you by your ISP to configure the WAN IP settings.
Obtain an IP address automatically
Use the following IP address:
WAN IP Address:
0.0.0.0
Enable NAT
MTU:
1492
(default: 1492)
< Back
Next >

On this screen, you have to make the settings for WAN IP. To get the IP address automatically, click the **Obtain an IP address automatically** radio button. Or click **Use the following IP address** button and enter the IP address for WAN interface.

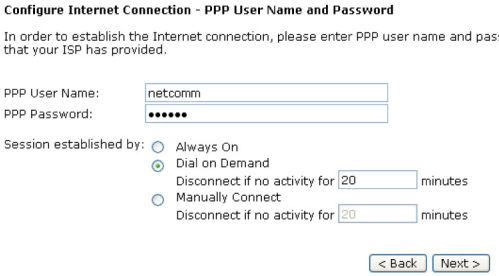
Check **Enable NAT** if you need.

MTU:

It means the maximum size of the packet that transmitted in the network. The packet of the data greater than the value set here will be divided into several packets for transmitting.

Type the value into the field of **MTU**. The default MTU value for PPPoE is 1492; while for PPPoA is 1500.

Click **Next** for the next procedure.


Configure Internet Connection - PPP User Name and Password
In order to establish the Internet connection, please enter PPP user name and password that your ISP has provided.
PPP User Name:
netcomm
PPP Password:
Session established by:
Always On
Dial on Demand
Disconnect if no activity for 20 minutes
Manually Connect
Disconnect if no activity for 20 minutes
< Back
Next >

PPP Username & PPP Password:

Key in the username and password that you received from your ISP. (e.g., hpotter/hogwarts)

Always On:

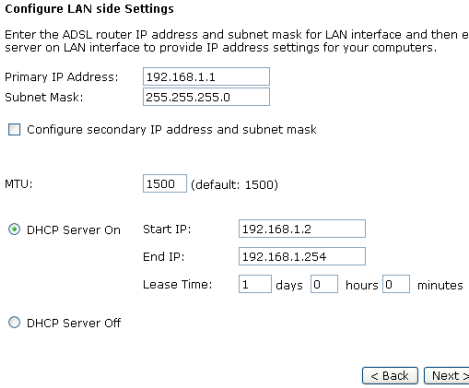
Select this item to make the connection active all the time.

Dial on Demand:

Select this item to make a connection automatically while in demand. Enter the timeout to cut off the network connection if there is no activity for this router.

Manually Connect:

Select this item to make a connection by pressing the **Connect** hyperlink on the **Advanced Setup-Internet-Connections** web page.



On the **Configure LAN side Settings** page, you have to fill in the data requested.

Primary IP Address & Subnet Mask:

Key in the information that offered by your ISP for the LAN connection.

Configure the secondary IP Address and Subnet Mask:

Check this box to set up a secondary IP Address to connect to your router if they are not included in the range that DHCP server accepts. See the next figure for the secondary IP address and subnet mask.

Secondary IP Address & Subnet Mask:

Key in the second IP address and the subnet mask received from the ISP for your LAN connection.

MTU: (refer to the WAN section)

The default **MTU** value for **LAN side Settings** is 1500. You may modify it if necessary.

DHCP Server On:

Check this item if DHCP service is needed on the LAN side. The router will assign IP address and gateway address for each of your PCs.

Start IP Address & End IP Address:

Enter the information needed.

Lease Time:

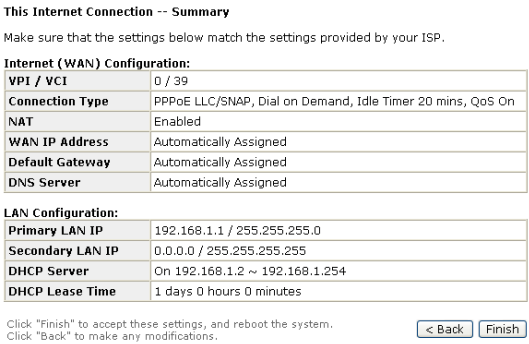
Key in the duration for the time. The default is 1day.

DHCP Server Off:

Check this item if DHCP service is not needed on the LAN.

On this web page, the primary IP address and subnet mask will be shown. You can modify them if needed.

Key in all the necessary settings and click **Next**.



This Internet Connection -- Summary

Make sure that the settings below match the settings provided by your ISP.

Internet (WAN) Configuration:

VPI / VCI	0 / 39
Connection Type	PPPoE LLC/SNAP, Dial on Demand, Idle Timer 20 mins, QoS On
NAT	Enabled
WAN IP Address	Automatically Assigned
Default Gateway	Automatically Assigned
DNS Server	Automatically Assigned

LAN Configuration:

Primary LAN IP	192.168.1.1 / 255.255.255.0
Secondary LAN IP	0.0.0.0 / 255.255.255.255
DHCP Server	On 192.168.1.2 ~ 192.168.1.254
DHCP Lease Time	1 days 0 hours 0 minutes

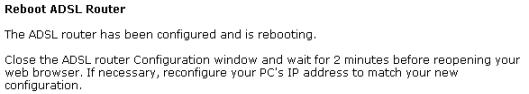
Click "Finish" to accept these settings, and reboot the system.
Click "Back" to make any modifications.

< Back | Finish

You can check the contents on the **Summary** page.

If you find anything incorrect, click **Back** to modify the settings.

If everything is OK, click **Finish** to accept these settings.



Reboot ADSL Router

The ADSL router has been configured and is rebooting.

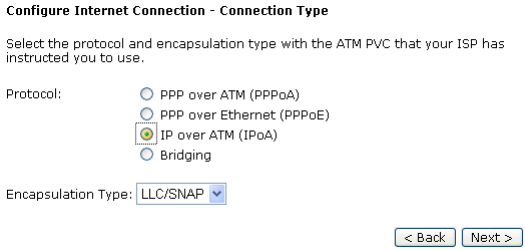
Close the ADSL router Configuration window and wait for 2 minutes before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

Now, the system will reboot to activate the new settings that you have set in this section.

Please wait for 2 minutes before restarting the router.

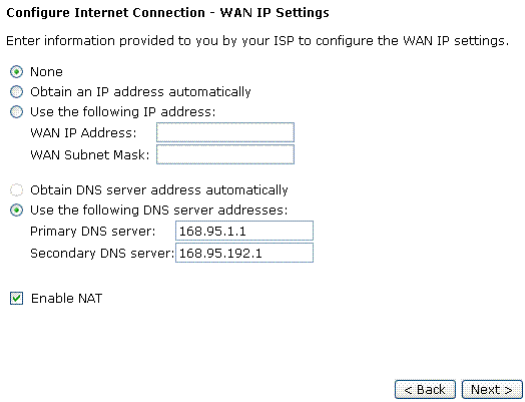
IP over ATM

If the type you have to choose is IP over ATM, please refer to the following information.


Configure Internet Connection - Connection Type
Select the protocol and encapsulation type with the ATM PVC that your ISP has instructed you to use.
Protocol:
PPP over ATM (PPPoA)
PPP over Ethernet (PPPoE)
IP over ATM (IPoA)
Bridging
Encapsulation Type:
LLC/SNAP
< Back
Next >

IPoA is an alternative of LAN emulation. It allows TCP/IP network to access ATM network and uses ATM quality of service's features.

Choose **IPoA** and click **Next**.


Configure Internet Connection - WAN IP Settings
Enter information provided to you by your ISP to configure the WAN IP settings.
None
Obtain an IP address automatically
Use the following IP address:
WAN IP Address:
WAN Subnet Mask:
Obtain DNS server address automatically
Use the following DNS server addresses:
Primary DNS server:
168.95.1.1
Secondary DNS server:
168.95.192.1
Enable NAT
< Back
Next >

None:

If it is not necessary to set the WAN IP address, please click this button.

Obtain an IP address automatically:

Click this button to allow the system to get an IP address automatically.

WAN IP Address & WAN Subnet Mask:

If you choose **Use the following IP address**, you have to enter the IP address and subnet mask information received from the ISP for the WAN interface.

Obtain DNS server address automatically:

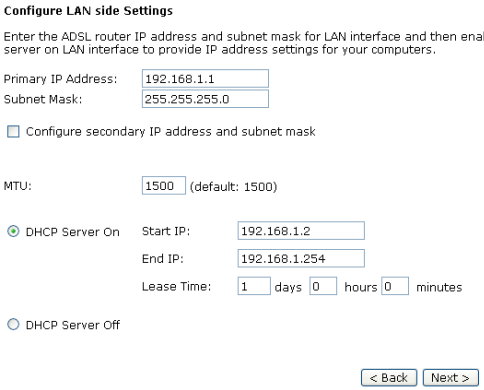
Only when you select **Obtain an IP address automatically** that this option is available. You may click this button to allow the system to get DNS server address automatically.

Use the following DNS server addresses:

Select this item to set the DNS server addresses manually, type the information provided by your ISP in the following **Primary DNS** and **Secondary DNS** server entries, e.g. 168.95.1.1 and 168.95.192.1.

Click **Enable NAT** if you want.

After setting up the WAN IP and DNS server information, click Next to open the following page.


Configure LAN side Settings
Enter the ADSL router IP address and subnet mask for LAN interface and then enable DHCP server on LAN interface to provide IP address settings for your computers.
Primary IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0
Configure secondary IP address and subnet mask
MTU: 1500 (default: 1500)
DHCP Server On
Start IP: 192.168.1.2
End IP: 192.168.1.254
Lease Time: 1 days 0 hours 0 minutes
DHCP Server Off
< Back
Next >

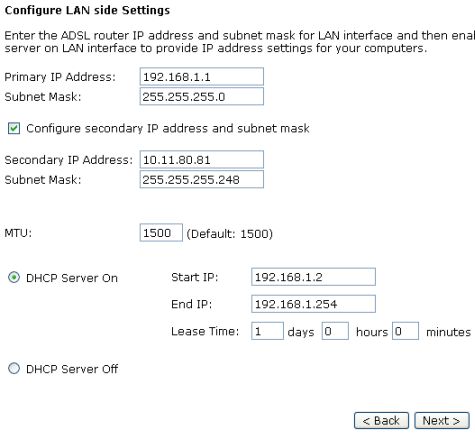
On the **Configure LAN side Settings** page, you have to fill in the data requested.

Primary IP Address & Subnet Mask:

Key in the information that offered by your ISP for the LAN connection, e.g., 192.168.1.1 for IP address and 255.255.255.0 for subnet mask.

MTU:

(Please refer to the PPPoA/ PPPoE section.) The default **MTU** setting here is 1500. You may modify it if necessary.


Configure LAN side Settings
Enter the ADSL router IP address and subnet mask for LAN interface and then enable DHCP server on LAN interface to provide IP address settings for your computers.
Primary IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0
Configure secondary IP address and subnet mask
Secondary IP Address: 10.11.80.81
Subnet Mask: 255.255.255.248
MTU: 1500 (Default: 1500)
DHCP Server On
Start IP: 192.168.1.2
End IP: 192.168.1.254
Lease Time: 1 days 0 hours 0 minutes
DHCP Server Off
< Back
Next >

Configure the secondary IP Address and Subnet Mask for LAN interface:

Check this box to set up a secondary IP Address to connect to your router if they are not included in the range that DHCP server accepts. You have to key in the information received from your ISP for the LAN connection, e.g., the secondary IP is 10.11.80.81 and the mask is 255.255.255.248 in the example illustrated in the figure.

DHCP Server On:

Check this item if DHCP service is needed on the LAN side. The router will assign IP address and gateway address for each of your PCs.

Start IP Address & End IP Address:

Enter the information needed.

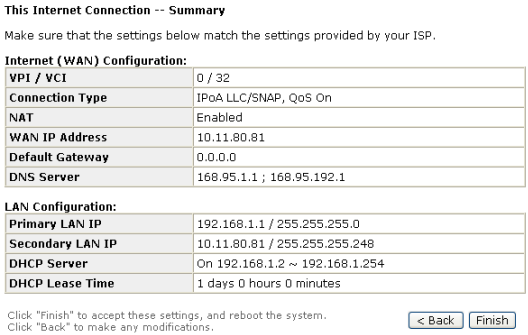
Lease Time:

Key in the duration for the time. The default is 1day.

DHCP Server Off:

Check this item if DHCP service is not needed on the LAN.

Key in all the necessary settings. Click **Next** for the coming page.



This Internet Connection -- Summary

Make sure that the settings below match the settings provided by your ISP.

Internet (WAN) Configuration:

VPI / VCI	0 / 32
Connection Type	IPoA LLC/SNAP, QoS On
NAT	Enabled
WAN IP Address	10.11.80.81
Default Gateway	0.0.0.0
DNS Server	168.95.1.1 ; 168.95.192.1

LAN Configuration:

Primary LAN IP	192.168.1.1 / 255.255.255.0
Secondary LAN IP	10.11.80.81 / 255.255.255.248
DHCP Server	On 192.168.1.2 ~ 192.168.1.254
DHCP Lease Time	1 days 0 hours 0 minutes

Click "Finish" to accept these settings, and reboot the system.
Click "Back" to make any modifications.

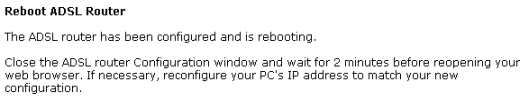
< Back | Finish

You can check the settings on the **Summary** page.

If you find anything incorrect, click **Back** to modify the settings.

If everything is OK, click **Finish** to accept these settings.

And the following page will appear.



Reboot ADSL Router

The ADSL router has been configured and is rebooting.

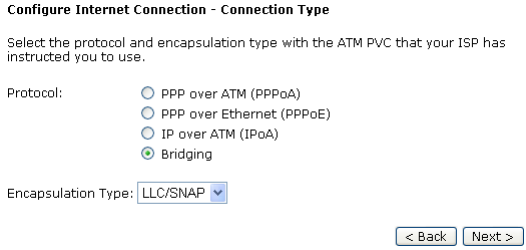
Close the ADSL router Configuration window and wait for 2 minutes before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

Now, the system will reboot to activate the new settings that you have set in this section.

Please wait for 2 minutes before restarting the router.

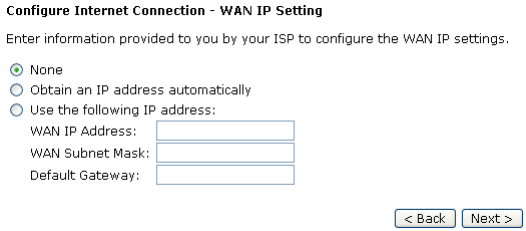
Bridging

If the mode you choose is **Bridging** (or **MER**), please refer to the following information.


Configure Internet Connection - Connection Type
Select the protocol and encapsulation type with the ATM PVC that your ISP has instructed you to use.
Protocol:
PPP over ATM (PPPoA)
PPP over Ethernet (PPPoE)
IP over ATM (IPoA)
Bridging
Encapsulation Type:
LLC/SNAP
< Back
Next >

The bridging mode can configure your router to send and receive packets between LAN and WAN interfaces. The WAN interface is ATM PVC; the LAN interface can be Ethernet, USB, or Wireless.

Choose **Bridging** and click **Next**.


Configure Internet Connection - WAN IP Setting
Enter information provided to you by your ISP to configure the WAN IP settings.
None
Obtain an IP address automatically
Use the following IP address:
WAN IP Address:
WAN Subnet Mask:
Default Gateway:
< Back
Next >

None:

If it is not necessary to set the WAN IP address, please click this button.

Obtain an IP address automatically:

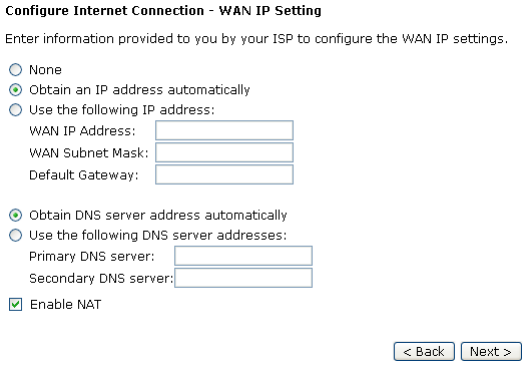
Click this button to allow the system to get an IP address automatically.

WAN IP Address, WAN Subnet Mask, and Default Gateway:

When choosing **Use the following IP address**, you have to key in the IP address, the subnet mask, and the default gateway provided by your ISP for the WAN interface.

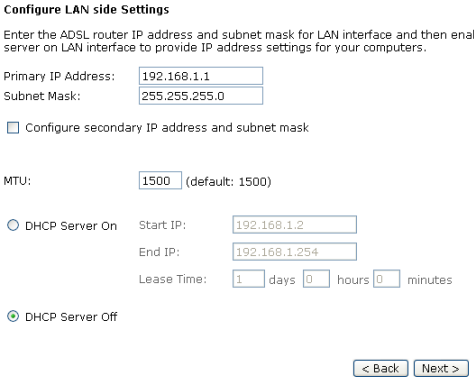
If you choose to obtain the IP address automatically or use specific IP address, you have to decide whether to select Obtain DNS server address automatically or Use the following DNS server address and enter the information provided by you ISP.

The default setting is none, if selecting **Obtain an IP address automatically** or **Use the following IP address**, the DNS setting appears, shown as the figure below.


Configure Internet Connection - WAN IP Setting
Enter information provided to you by your ISP to configure the WAN IP settings.
None
Obtain an IP address automatically
Use the following IP address:
WAN IP Address:
WAN Subnet Mask:
Default Gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Primary DNS server:
Secondary DNS server:
Enable NAT
< Back
Next >

Check **Enable NAT** if necessary.

Press **Next** to continue.



Primary IP Address & Subnet Mask:

Key in the IP address and the subnet mask that provided by your ISP for LAN interface, e.g., 192.168.1.1 and 255.255.255.0, respectively.

MTU:

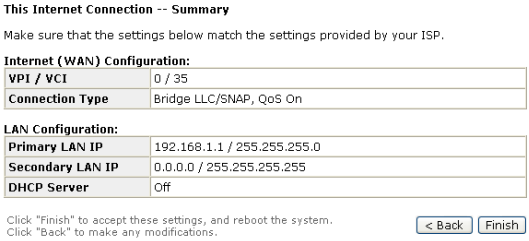
Please refer to PPPoA/ PPPoE.

DHCP Server On:

Check this item if DHCP service is needed on the LAN. The router will assign IP address and gateway address for each of your PCs. Enter the information for **Start IP**, **End IP** and **Lease Time** if you enable this function. The default value for lease time is one day.

DHCP Server Off:

Check this item if DHCP service is not needed on the LAN; like our example.



This Internet Connection -- Summary

Make sure that the settings below match the settings provided by your ISP.

Internet (WAN) Configuration:

VPI / VCI	0 / 35
Connection Type	Bridge LLC/SNAP, QoS On

LAN Configuration:

Primary LAN IP	192.168.1.1 / 255.255.255.0
Secondary LAN IP	0.0.0.0 / 255.255.255.255
DHCP Server	Off

Click "Finish" to accept these settings, and reboot the system.
Click "Back" to make any modifications.

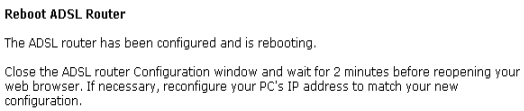
< Back | Finish

You can check the settings on the **Summary** page now.

If you find anything incorrect, click **Back** to modify the settings.

If everything is OK, click **Finish** to accept these settings.

And the following page will appear.



Reboot ADSL Router

The ADSL router has been configured and is rebooting.

Close the ADSL router Configuration window and wait for 2 minutes before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

Now, the system will reboot to activate the new settings that you have done in this section.

Please wait for 2 minutes before restarting the router.

Status

Overview

Device Information

This information reflects the current status of your ADSL router.

System Up Time	00:00:56:13
ADSL Speed (DS/US)	7616/832 Kbps
LAN IP Address	192.168.1.1
Default Gateway	10.11.95.233
Primary DNS server	168.95.192.1
Secondary DNS server	168.95.1.1

Firmware Version	3.28p
Boot Loader Version	1.0.37-0.6.5
ADSL Driver Version	A2pB021.d17m
Ethernet MAC Address	00:11:F5:61:5F:9A

This page displays the current status for the ADSL connection, including the period of activating the router, ADSL speed, and the information about LAN IP address, default gateway, DNS server, firmware version, boot loader version, wireless driver version, wireless BSSID, and Ethernet MAC address. The system status will be different according to the settings that you configured in the web pages.

ADSL Line

ADSL Line Status

Current ADSL line status is displayed as the below.

Line Mode	G.DMT	**Line State**	Show Time
Latency Type	Interleave	**Line Up Time**	00:01:21:44
Line Coding	Trellis On	**Line Up Count**	1

Statistics	**Downstream**	**Upstream**
Line Rate	7616 Kbps	832 Kbps
Attainable Line Rate	11328 Kbps	1224 Kbps
Noise Margin	22.2 dB	14.0 dB
Line Attenuation	2.0 dB	2.0 dB
Output Power	7.7 dBm	11.9 dBm

More Information

ADSL BER Test

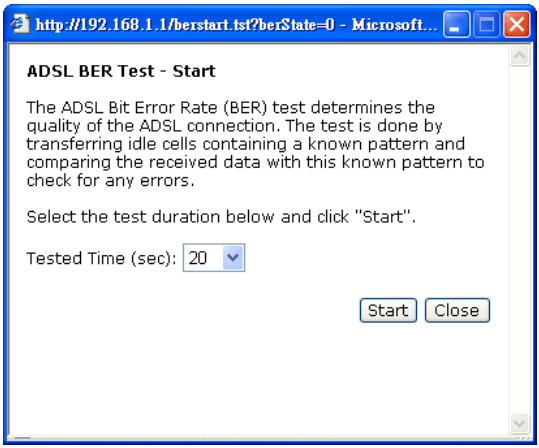
This page shows all information for ADSL.

For knowing the quality of the ADSL connection, please click **ADSL BER Test** button to have advanced information.

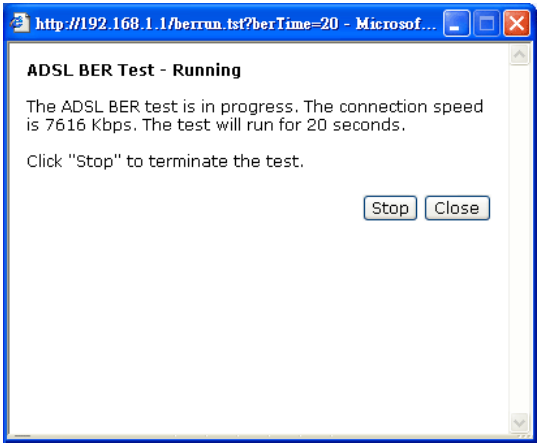
Click **More Information** hyperlink to see more detailed information about ADSL Line Status.

ADSL BER Test

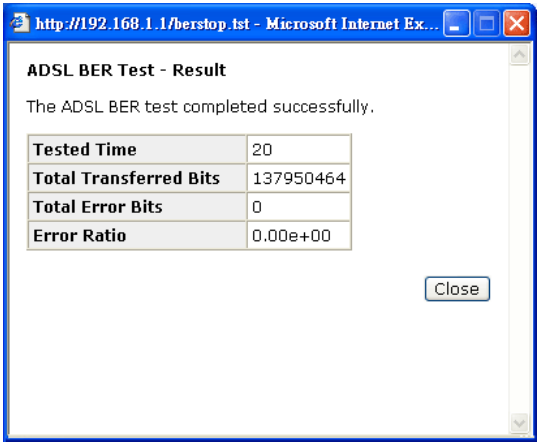
This test determines the quality of the ADSL connection. It is done by transferring idle cells containing a known pattern and comparing the received data with this known pattern to check for errors.


http://192.168.1.1/berstart.tst?berState=0 - Microsoft...
ADSL BER Test - Start
The ADSL Bit Error Rate (BER) test determines the quality of the ADSL connection. The test is done by transferring idle cells containing a known pattern and comparing the received data with this known pattern to check for any errors.
Select the test duration below and click "Start".
Tested Time (sec): 20
Start
Close

After selecting the test duration time and click **Start**, the following dialog appears to tell you the test is running. You can stop the test by clicking **Stop** or close this dialog window by pressing **Close**.


http://192.168.1.1/berrun.tst?berTime=20 - Microsof...
ADSL BER Test - Running
The ADSL BER test is in progress. The connection speed is 7616 Kbps. The test will run for 20 seconds.
Click "Stop" to terminate the test.
Stop
Close

When the test is over, the result will be shown on the following dialog window for your reference.



Click **Close** to close this window.

Internet Connection

This page displays the connection information for your router, such as the PVC name, VPI/VCI value, service category, protocol, invoking NAT and QoS or not, IP address, linking status, and so on.

Internet Connection

Current Internet connections are listed below.

PVC Name	VPI/VCI	Category	Protocol	NAT	QoS	WAN IP Address	Status / Online Time
pppoe_0_39_1	0/39	UBR	PPPoE LLC/SNAP	On	On	10.11.65.13	Up 00:00:43:40

Traffic Statistics

This table shows the records of data going through the LAN and WAN interface. For each interface, cumulative totals are displayed for Received and Transmitted.

You may click Reset to reset the amount.

Traffic Statistics

The statistics of user data going through your ADSL router are listed below.

Interface	Received				Transmitted			
	Bytes	Packets	Errors	Drops	Bytes	Packets	Errors	Drops
Ethernet	2118	16	0	0	4853	16	0	0
USB	0	0	0	0	0	0	0	0
Wireless	0	0	0	0	0	0	0	0
WAN	192	2	0	0	192	2	0	0

Reset

DHCP Table

This table shows all DHCP clients who get their IP addresses from your ADSL Router. For each DHCP client, it shows the **Host Name**, **MAC Address**, **IP Address** and the **Lease Time**.

DHCP Table

Those devices which get their IP addresses from your DSL Router are listed below.

Host Name	MAC Address	IP Address	Lease Time
CN	00:C1:26:0A:69:2B	192.168.1.2	00:23:55:31

Wireless Clients (NB6W and NB6Plus4W only)

This table shows the MAC address for all of the wireless LAN clients currently associated to your ADSL Router.

Wireless Clients Table

All of wireless LAN clients currently associated to your ADSL router are listed below.

NOTE: The list below might include wireless clients which are no longer connected to your ADSL router. You need to wait for a few seconds for the list to be fully updated.

MAC Address	On-line Time

Routing Table

This table shows the routing rules that your router uses.

Routing Table

All of current routing rules in your ADSL router are listed below.

Destination	Netmask	Gateway	Interface	Metric
10.11.95.233	255.255.255.255	0.0.0.0	pppoe_0_39_1	0
192.168.1.0	255.255.255.0	0.0.0.0	br0	0
0.0.0.0	0.0.0.0	10.11.95.233	pppoe_0_39_1	0

ARP Table

This table shows the IP address record for IP-to-Physical translation in your router.

ARP Table

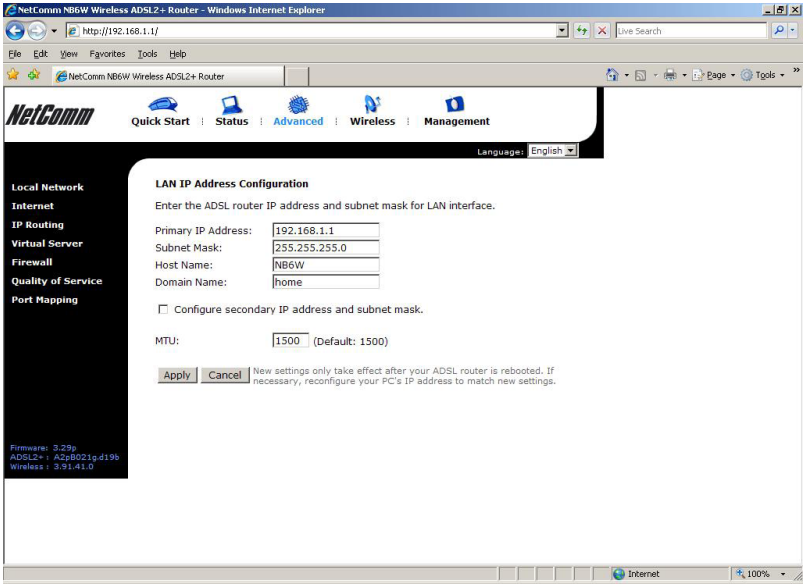
The IP-to-Physical address translation entries recorded in your ADSL router are listed below.

IP address	Physical Address	Interface	Type
192.168.1.2	00:C1:26:0A:69:2B	br0	Dynamic

Advanced Setup

Local Network – IP Address

This page is the same as you can see on the Configure LAN side Settings page while running the Quick Setup. It allows you to set IP Address and Subnet Mask values for LAN interface.



Primary IP Address:

Key in the first IP address that you received from your ISP for the LAN connection.

Subnet Mask:

Key in the subnet mask that you received from your ISP for the LAN connection.

Host Name:

List the host name of this device.

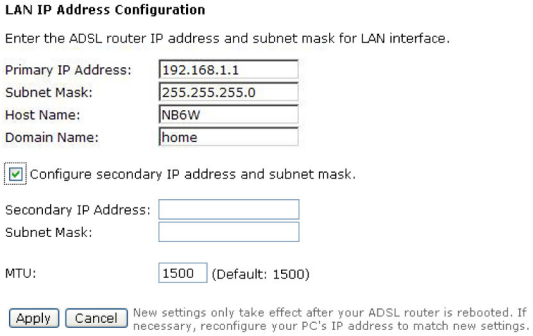
Domain Name:

List the name of the domain.

Configure the secondary IP Address and Subnet Mask:

Check this box to enter another set of IP Address and Subnet Mask to connect to your router if they are not included in the range that DHCP server accepts.

After checking this box, the secondary IP address and subnet mask entries will show up, as shown below.



Secondary IP Address & Subnet Mask:

Enter the information provided by your ISP for your LAN connection.

MTU:

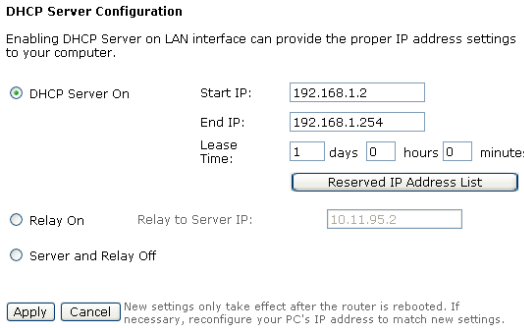
It means the maximum size of the packet that transmitted in the network. The packet of the data greater than the number set here will be divided into several packets for transmitting. Type the value into the field of **MTU**. The default setting for LAN configuration is 1500.

Apply:

Click this button to activate the settings listed above.

Local Network – DHCP Server

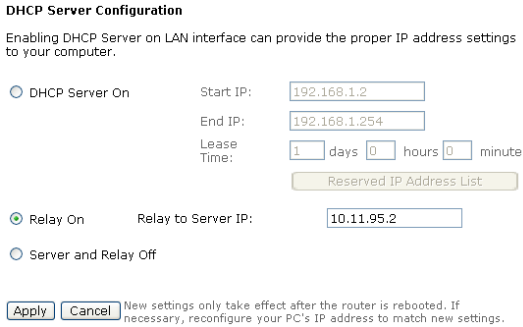
This allows you to set DHCP server on LAN interface.


DHCP Server Configuration
Enabling DHCP Server on LAN interface can provide the proper IP address settings to your computer.
DHCP Server On
Start IP:
192.168.1.2
End IP:
192.168.1.254
Lease Time:
1 days 0 hours 0 minutes
Reserved IP Address List
Relay On
Relay to Server IP:
10.11.95.2
Server and Relay Off
Apply
Cancel
New settings only take effect after the router is rebooted. If necessary, reconfigure your PC's IP address to match new settings.

DHCP Server On:

Check this item if DHCP service is needed on the LAN. The router will assign IP address and gateway address for each of your PCs.

You have to key in **Start IP Address**, **End IP Address**, and **Lease Time**. The default lease time is 1day.


DHCP Server Configuration
Enabling DHCP Server on LAN interface can provide the proper IP address settings to your computer.
DHCP Server On
Start IP:
192.168.1.2
End IP:
192.168.1.254
Lease Time:
1 days 0 hours 0 minutes
Reserved IP Address List
Relay On
Relay to Server IP:
10.11.95.2
Server and Relay Off
Apply
Cancel
New settings only take effect after the router is rebooted. If necessary, reconfigure your PC's IP address to match new settings.

Relay On:

Click this button to have a relay setting. And type the Server IP in the IP field.

When the DHCP server is served by another device rather than the router itself, you can relay to that specific server and enter the IP address of it, as 10.11.95.2 in our example.

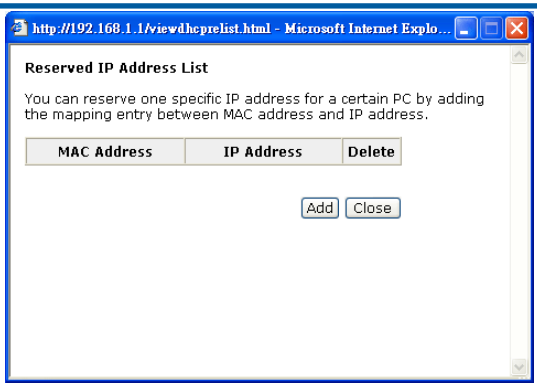
Server and Relay Off:

Check this item if DHCP service isn't needed on the LAN.

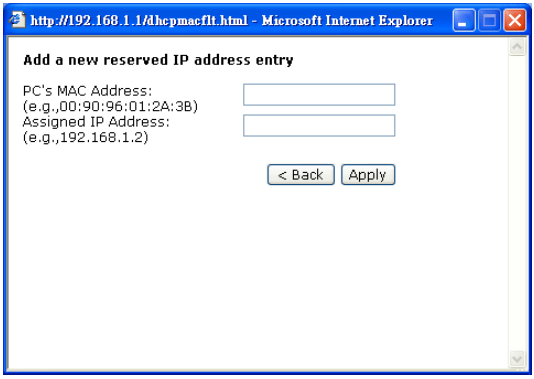
Apply:

Click this button to activate the settings listed above.

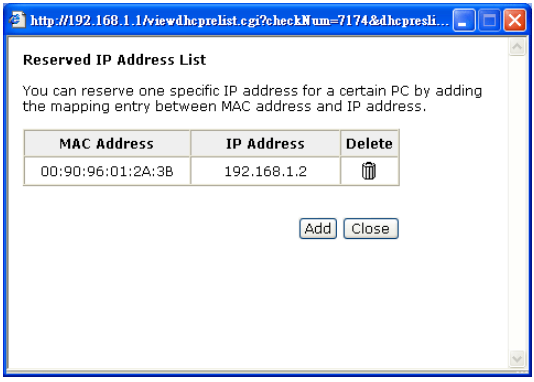
You can reserve one specific IP address for a certain PC for particular purpose. Simply add a mapping entry of MAC address & IP address for that PC by pressing the **Reserved IP Address List** button. The following window will appear.


http://192.168.1.1/viewdhcprelist.html - Microsoft Internet Explo...
Reserved IP Address List
You can reserve one specific IP address for a certain PC by adding the mapping entry between MAC address and IP address.
MAC Address
IP Address
Delete
Add
Close

Click the **Add** button to open another dialog window, shown below. On **PC's MAC Address** and **Assigned IP Address** boxes, please type the correct information according to your need and click **Apply**.



The information added will be shown on the window right away, as below. That is, the specified address will be reserved and not be assigned by DHCP for other computer(s).

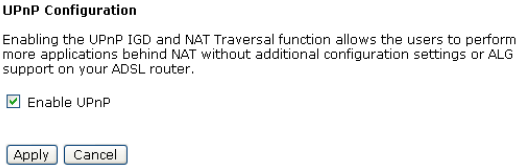


You may click **Add** button to add another set or click **Close** to exit.

Local Network – UPnP

The UPnP is only available for Windows XP. If you are not a Windows XP user, you may ignore this page.

Enabling the UPnP IGD and NAT traversal function allows the users to perform more applications behind NAT without additional configuration settings or ALG support on your ADSL Router.


UPnP Configuration
Enabling the UPnP IGD and NAT Traversal function allows the users to perform more applications behind NAT without additional configuration settings or ALG support on your ADSL router.
Enable UPnP
Apply
Cancel

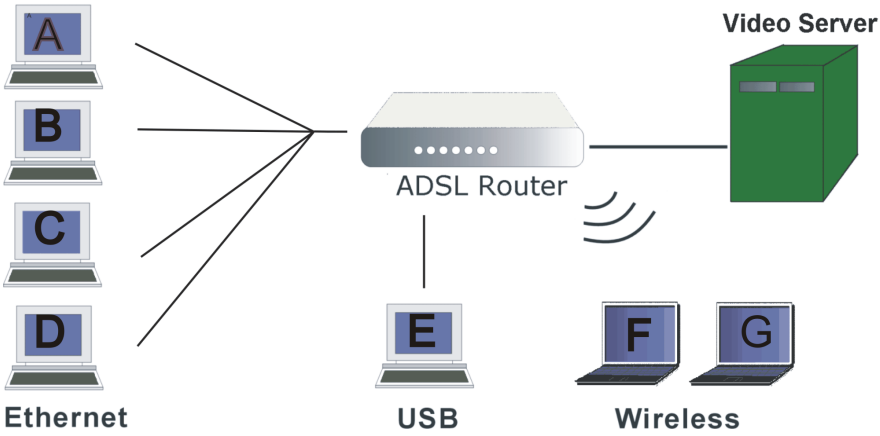
You can enable the UPnP function through this web page by checking **Enable UPnP** and press **Apply**.

Local Network – IGMP Snooping

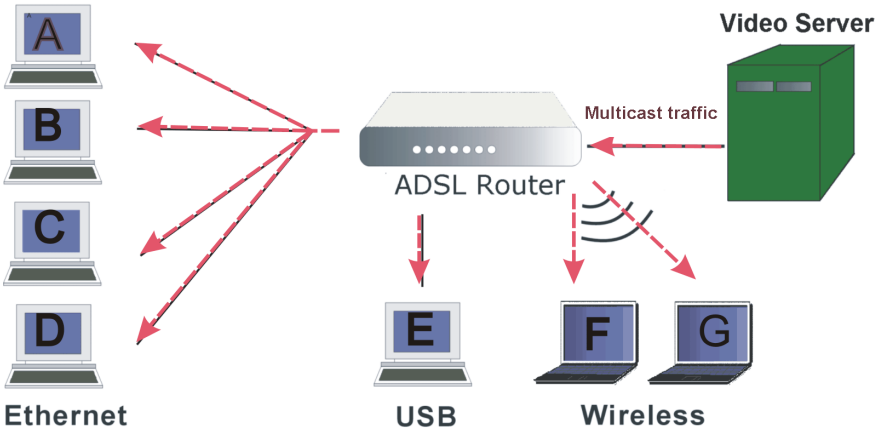
Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender to 1 recipient) or Broadcast (1 sender to everyone on the network). Multicast delivers IP packets to just a group of hosts on the network.

Without IGMP snooping, multicast traffic is treated in the same manner as broadcast traffic, that is, it is forwarded to all ports. With IGMP snooping, multicast traffic of a group is only forwarded to ports that have members of that group. IGMP snooping generates no additional network traffic, allowing you to significantly reduce multicast traffic passing through your switch.

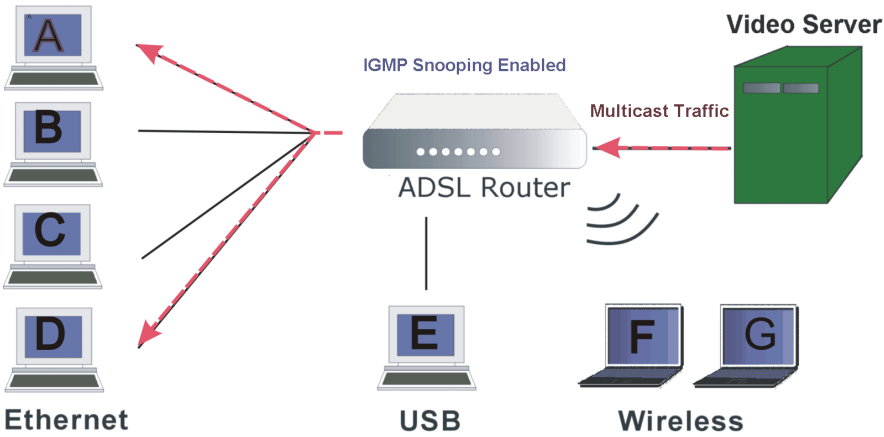
The figure below shows a simple network connected via this ADSL router. There are four Ethernet clients, one using USB, and two wireless clients.



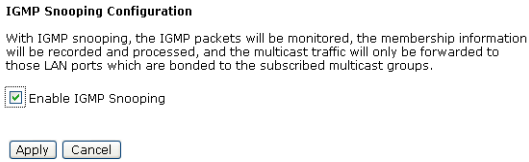
Now suppose the video server is the multicast transmitter and host A and D are multicast receivers. If we do not turn on the IGMP snooping function, the router will forward the multicast traffic to all hosts on all interfaces and consequently block and interrupt the traffic of USB and wireless users, shown as the following figure.



When IGMP snooping is invoked, it makes the system aware to establish the best path for multicast service to save LAN bandwidth. Refer the figure below, just as desired, only host A and D will actually receive multicast traffic when IGMP snooping is enabled.



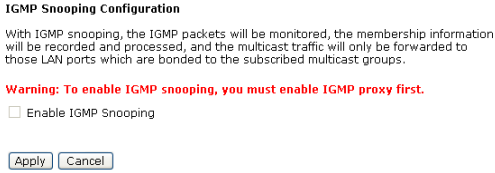
While IGMP snooping is enabled, the IGMP packets will be monitored, the membership information will be recorded and processed, and the multicast traffic will only be forwarded to those LAN interfaces, such as Ethernet, Wireless, and USB, which are bonded to the subscribed multicast groups. Thus it helps to save the bandwidth and helps the devices to perform more effectively.


IGMP Snooping Configuration
With IGMP snooping, the IGMP packets will be monitored, the membership information will be recorded and processed, and the multicast traffic will only be forwarded to those LAN ports which are bonded to the subscribed multicast groups.
Enable IGMP Snooping
Apply
Cancel

Check Enable IGMP Snooping and click Apply to invoke this function.

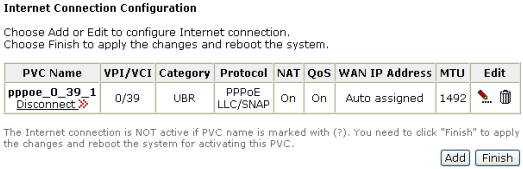
If the PVC you're using is NAT enabled, remember to turn on the IGMP Proxy at the same time. Please refer to Internet – IGMP Proxy for more information.

Note that the IGMP proxy must be enabled first. If the IGMP Snooping function is not available as shown in the following figure, you have to enable the IGMP Proxy first.


IGMP Snooping Configuration
With IGMP snooping, the IGMP packets will be monitored, the membership information will be recorded and processed, and the multicast traffic will only be forwarded to those LAN ports which are bonded to the subscribed multicast groups.
Warning: To enable IGMP snooping, you must enable IGMP proxy first.
Enable IGMP Snooping
Apply
Cancel

Internet – Connections

To set WAN settings for each service, please open **Advanced** – **Internet.** This page allows you to edit, to remove, or to add WAN settings.

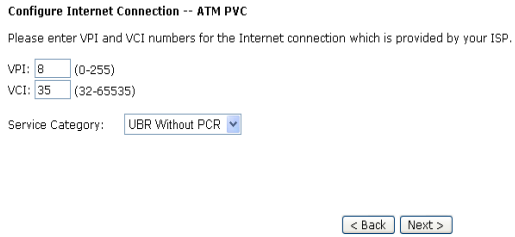


If you click the **Connect** hyperlink under the PVC Name item, the system will connect to WAN automatically. If the WAN connection is OK, you can check the detailed information directly.

You can add new PVC(s) by clicking the **Add** button, edit the settings for the present PVC by clicking in the **Edit** column, or delete the existing PVC by pressing icon.

Adding a New One

To add a new WAN connection, please click the **Add** button. The following screen appears.


Configure Internet Connection -- ATM PVC
Please enter VPI and VCI numbers for the Internet connection which is provided by your ISP.
VPI: 8 (0-255)
VCI: 35 (32-65535)
Service Category: UBR Without PCR
< Back
Next >

VPI (Virtual Path Identifier):

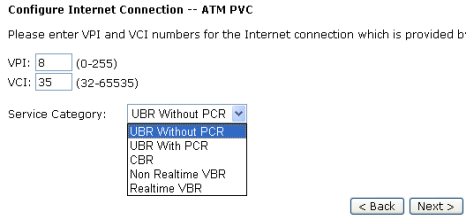
Identifies the virtual path between endpoints in an ATM network. The valid range is from 0 to 255. Please refer to the value that your ISP provides.

VCI (Virtual Channel Identifier):

Identifies the virtual channel endpoints in an ATM network. The valid range is from 32 to 65535 (1 to 31 is reserved for well-known protocols). Please refer to the value that your ISP provides.

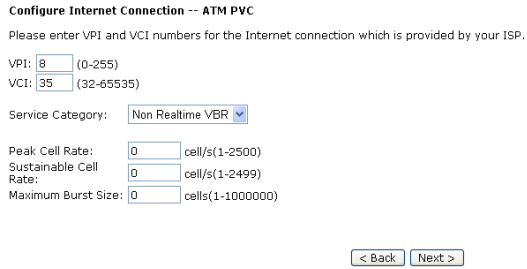
Service Category:

It decides the size and rate for the packets of the data in different service type. There are five categories provided here for your selection, shown as the drop-down menu below.


Configure Internet Connection -- ATM PVC
Please enter VPI and VCI numbers for the Internet connection which is provided by your ISP.
VPI: 8 (0-255)
VCI: 35 (32-65535)
Service Category: UBR Without PCR
UBR Without PCR
UBR With PCR
CBR
Non Realtime VBR
Realtime VBR
< Back
Next >

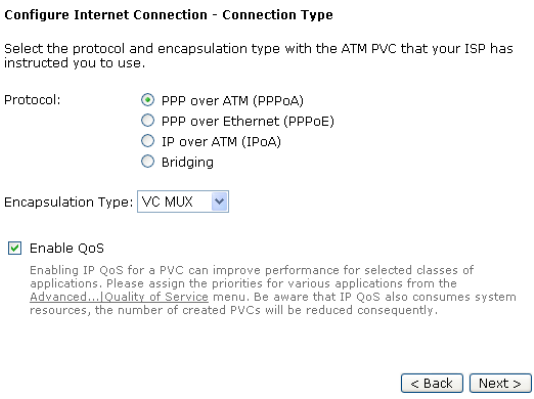
If you select **UBR with PCR** or **CBR**, you have to offer the value for the peak cell rate.

If you choose **Non Realtime VBR**, or **Realtime VBR**, you have to key in the value for the peak cell rate, sustainable cell rate, and maximum burst size.


Configure Internet Connection -- ATM PVC
Please enter VPI and VCI numbers for the Internet connection which is provided by your ISP.
VPI: 8 (0-255)
VCI: 35 (32-65535)
Service Category: Non Realtime VBR
Peak Cell Rate: 0 cell/s(1-2500)
Sustainable Cell Rate: 0 cell/s(1-2499)
Maximum Burst Size: 0 cells(1-1000000)
< Back
Next >

As you can see above, the range for **Peak Cell Rate** is from 1 to 2500; the value for **Sustainable Cell Rate** ranges from 1 to 2499 and must be smaller than Peak Cell Rate, and the range for **Maximum Burst Size** is from 1 to 1000000.

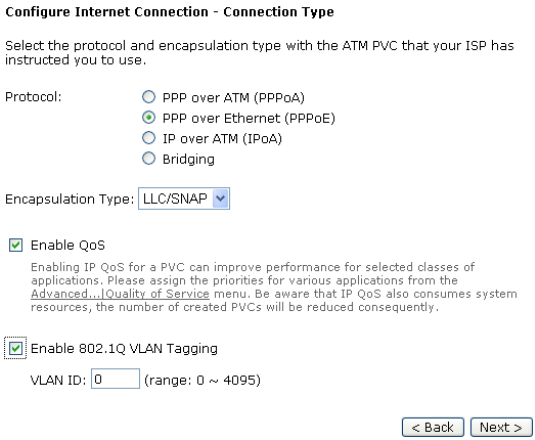
After pressing **Next**, you will see the web page below. Choose the protocol that you would like to use. (Here provides the example for PPPoA.)


Configure Internet Connection - Connection Type
Select the protocol and encapsulation type with the ATM PVC that your ISP has instructed you to use.
Protocol:
PPP over ATM (PPPoA)
PPP over Ethernet (PPPoE)
IP over ATM (IPoA)
Bridging
Encapsulation Type: VC MUX
Enable QoS
Enabling IP QoS for a PVC can improve performance for selected classes of applications. Please assign the priorities for various applications from the Advanced...|Quality of Service menu. Be aware that IP QoS also consumes system resources, the number of created PVCs will be reduced consequently.
< Back
Next >

Please refer to Quick Setup for more information if you don't know how to set the configuration.

You can check **Enable QoS** to improve performance for selected applications. More detailed information for QoS will be introduced in later instruction.

If you choose **PPPoE** (or **Bridging**), you will see the option for **802.1Q VLAN Tagging**.


Configure Internet Connection - Connection Type
Select the protocol and encapsulation type with the ATM PVC that your ISP has instructed you to use.
Protocol:
PPP over ATM (PPPoA)
PPP over Ethernet (PPPoE)
IP over ATM (IPoA)
Bridging
Encapsulation Type: LLC/SNAP
Enable QoS
Enabling IP QoS for a PVC can improve performance for selected classes of applications. Please assign the priorities for various applications from the Advanced...|Quality of Service menu. Be aware that IP QoS also consumes system resources, the number of created PVCs will be reduced consequently.
Enable 802.1Q VLAN Tagging
VLAN ID: 0 (range: 0 ~ 4095)
< Back
Next >

802.1Q VLAN Tagging:

802.1Q-compliant switch ports can be configured to transmit tagged or untagged frames. A tag field containing VLAN (and/or 802.1p priority) information can be inserted into an Ethernet frame. If a port has an 802.1Q-compliant device attached (such as another switch), these tagged frames can carry VLAN membership information between switches, thus letting a VLAN span multiple switches. However, it is important for network administrators to ensure ports with non-802.1Q-compliant devices attached are configured to transmit untagged frames. Many NICs for PCs and printers are not 802.1Q-compliant. If they receive a tagged frame, they will not understand the VLAN tag and will drop the frame. Also, the maximum legal Ethernet frame size for tagged frames was increased in 802.1Q (and its companion, 802.3ac) from 1,518 to 1,522 bytes.

After checking **Enable 802.1Q VLAN Tagging**, you will have to enter a **VLAN ID**, as shown.

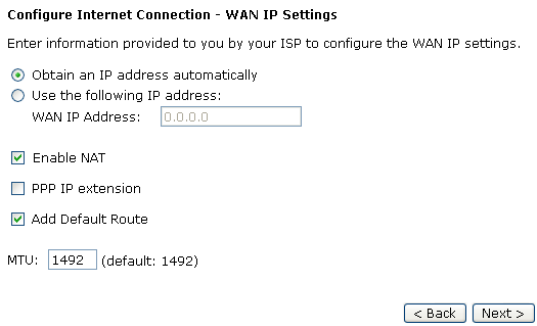
VLAN ID:

The VLAN Identifier is a 12 bit field. It uniquely identifies the VLAN to which the frame belongs to and can have a value between 0 and 4095.

Notice that **802.1Q VLAN Tagging** function can only be invoked under **PPPoE** and **Bridging Mode**; the system will not provide this option while setting **PPPoA** or **IPoA** mode.

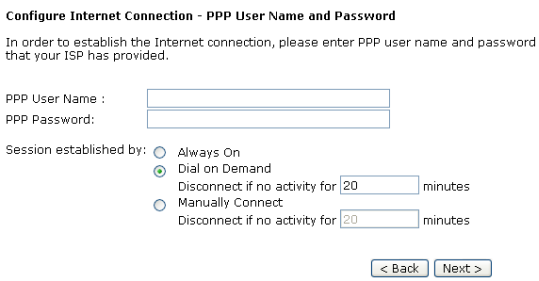
Click **Next** to continue.

The WAN IP settings page will differ slightly according to the protocol that you choose. This graphic is the one that you will see if you choose the PPPoE mode in the previous step. You can select **Enable NAT** or **PPP IP extension** according to your needs. And you can also change the **MTU** value.


Configure Internet Connection - WAN IP Settings
Enter information provided to you by your ISP to configure the WAN IP settings.
Obtain an IP address automatically
Use the following IP address:
WAN IP Address: 0.0.0.0
Enable NAT
PPP IP extension
Add Default Route
MTU: 1492 (default: 1492)
< Back
Next >

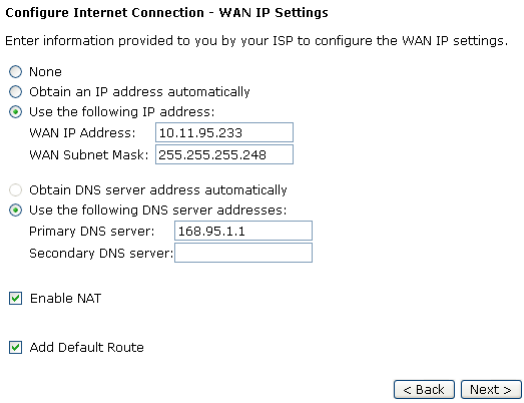
Add Default Route:

Check this item to add a default route.


Configure Internet Connection - PPP User Name and Password
In order to establish the Internet connection, please enter PPP user name and password that your ISP has provided.
PPP User Name :
PPP Password:
Session established by:
Always On
Dial on Demand
Disconnect if no activity for 20 minutes
Manually Connect
Disconnect if no activity for 20 minutes
< Back
Next >

The next figure following the WAN IP Settings in the PPPoA/ PPPoE mode is shown at the right. You may refer to the **Quick Setup** section for further information.

If you choose **IP over ATM** from the **Connection Type** web page, you will get a web page as the figure.


Configure Internet Connection - WAN IP Settings
Enter information provided to you by your ISP to configure the WAN IP settings.
None
Obtain an IP address automatically
Use the following IP address:
WAN IP Address: 10.11.95.233
WAN Subnet Mask: 255.255.255.248
Obtain DNS server address automatically
Use the following DNS server addresses:
Primary DNS server: 168.95.1.1
Secondary DNS server:
Enable NAT
Add Default Route
< Back
Next >

You may refer to **Quick Start** – **Connection Type** – **IPoA** section for more information.

Add Default Route:

Check this item to add a default IPoA route onto the routing table.

After rebooting your router, the default route will be shown on the **Routing Table** under **Status** menu, you may check it.

Routing Table

All of current routing rules in your ADSL router are listed below.

Destination	Netmask	Gateway	Interface	Metric
10.11.95.233	255.255.255.255	0.0.0.0	pppoe_0_39_1	0
10.11.95.232	255.255.255.248	0.0.0.0	ipoa_0_32	0
192.168.1.0	255.255.255.0	0.0.0.0	br0	0
0.0.0.0	0.0.0.0	0.0.0.0	ipoa_0_32	1

If you choose Bridging from the Connection Type web page, you will get a web page as below.

Configure Internet Connection - WAN IP Setting

Enter information provided to you by your ISP to configure the WAN IP settings.

- (•) None
- ( ) Obtain an IP address automatically
- ( ) Use the following IP address:

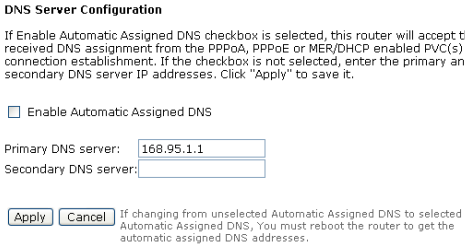
WAN IP Address:
WAN Subnet Mask:
Default Gateway:

< Back | Next >

Please refer to Quick Setup for more information.

Internet – DNS Server

If **Enable Automatic Assigned DNS** checkbox is selected, this router will accept the **first** received DNS assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s) during the connection establishment. If the checkbox is not selected, it is necessary for you to enter the primary and optional secondary DNS server IP addresses. Finish your setting and click the **Apply** button to save it and invoke it.


DNS Server Configuration
If Enable Automatic Assigned DNS checkbox is selected, this router will accept the first received DNS assignment from the PPPoA, PPPoE or MER/DHCP enabled PVC(s) during the connection establishment. If the checkbox is not selected, enter the primary and optional secondary DNS server IP addresses. Click "Apply" to save it.
Enable Automatic Assigned DNS
Primary DNS server: 168.95.1.1
Secondary DNS server:
Apply
Cancel
If changing from unselected Automatic Assigned DNS to selected Automatic Assigned DNS, You must reboot the router to get the automatic assigned DNS addresses.

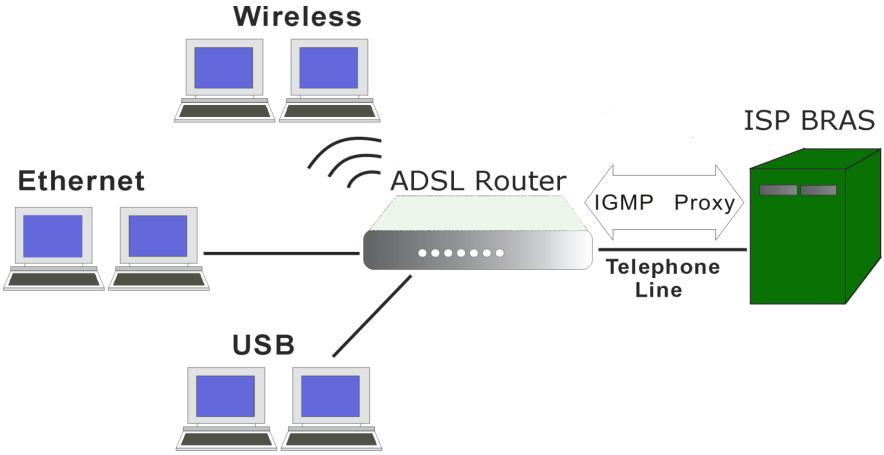
Enable Automatic Assigned DNS:

Check this box to enable this function, or uncheck this box to disable it. The default setting is checked. When this function is disabled, you have to offer the **Primary DNS server** and **Secondary DNS server**.

If you are satisfied with the settings, click **Apply**.

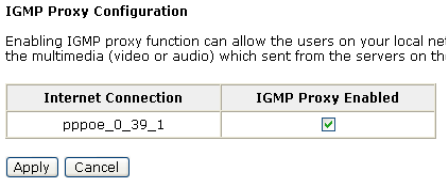
Internet – IGMP Proxy

The Internet Group Management Protocol (IGMP) is an Internet protocol that provides a way for an Internet computer to report its multicast group membership to adjacent routers.



The hosts interact with the system through the exchange of IGMP messages. When you want to configure IGMP proxy, the system will interact with other routers through the exchange of IGMP messages. However, when acting as the proxy, the system performs the host portion of the IGMP task as follows:

- When being queried, the system will send membership reports to the group.
- When one of the hosts joins a multicast address group which none of other hosts belongs to, the system will send unsolicited membership reports to that group.
- When the last host in a particular multicast group leaves the group, the system will send a leave group membership report to the router's group.


IGMP Proxy Configuration
Enabling IGMP proxy function can allow the users on your local network to play the multimedia (video or audio) which sent from the servers on the Internet.
Internet Connection
IGMP Proxy Enabled
pppoe_0_39_1
Apply
Cancel

Internet Connection:

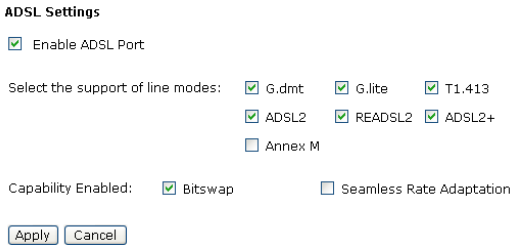
This field displays the internet connection(s) that set in this router.

IGMP Proxy Enabled:

Check this box to enable this function or uncheck this box to disable this function.

After finish the settings, click **Apply**.

To invoke the IGMP Snooping function, the IGMP Proxy must be enabled first.



Enable ADSL Port:

Check this box to enable this function. It simply invokes the line mode that you choose here for the router.

Select the support of line modes:

There are several selections, and you may select them according to the line modes supported by your ISP and your needs.

Capability Enabled:

Two items are provided here for you to choose.

Bitswap:

It is a mandatory receiver initiated feature to maintain the operating conditions of the modem during changing environment conditions. It reallocates the data bits and power among the allowed carriers without modification of the higher layer control parameters in the ATU. After a bit swapping reconfiguration, the total data rate and the data rate on each latency path is unchanged. Check this box to enable the function. If not, uncheck this box to close the function.

Seamless Rate Adaptation:

It enables the ADSL2/ ADSL2+ Router to change the data rate of the connection while in operation without any service interruption or bit errors. Check this box to enable the function. If not, uncheck this box to close the function.

IP Routing – Static Route

The table shows all static route status and allows you to add new static IP route or delete static route. A Static IP Routing is a manually defined path, which determines the data transmitting route. If your local network is composed of multiple subnets, you may want to specify a routing path to the routing table.

Destination Network Address:

Display the IP address that the data packets are to be sent.

Netmask, Gateway, WAN Interface:

Display the subnet mask, gateway, and WAN interface information that the transmitting data will pass through.

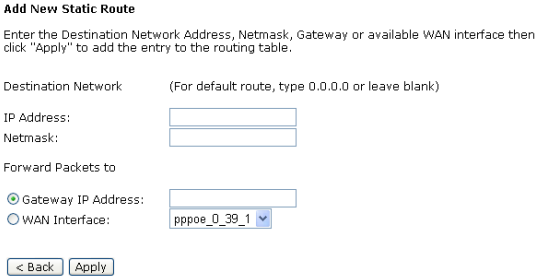
Delete:

Allow you to remove the static route settings.

This page shows all the routing table of data packets going through your ADSL Router.

Adding a New One

To add a static route, please click **Add**. Type the destination network address, subnet mask and gateway that you received from the ISP and click **Apply**.


Add New Static Route
Enter the Destination Network Address, Netmask, Gateway or available WAN interface then click "Apply" to add the entry to the routing table.
Destination Network
(For default route, type 0.0.0.0 or leave blank)
IP Address:
Netmask:
Forward Packets to
Gateway IP Address:
WAN Interface:
pppoe_0_39_1
< Back
Apply

IP Address:

The destination IP address of the network indicates where data packets are to be sent. You may specify an IP, type 0.0.0.0, or leave it blank.

Netmask:

Enter the subnet mask that you got from the ISP, type 0.0.0.0 or leave it blank.

Gateway IP Address:

Click this button to forward packets to the specific gateway. Key in the gateway IP address that you want to use.

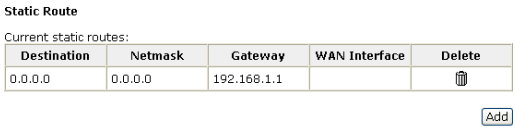
WAN Interface:

Click this button to forward packets to a specific WAN interface. Choose one from the drop-down menu.

E.g., type 192.168.1.1 in the field of the gateway IP address and leave the destination network blank.

Click **Apply** to view the routing result.

Remove Static Route

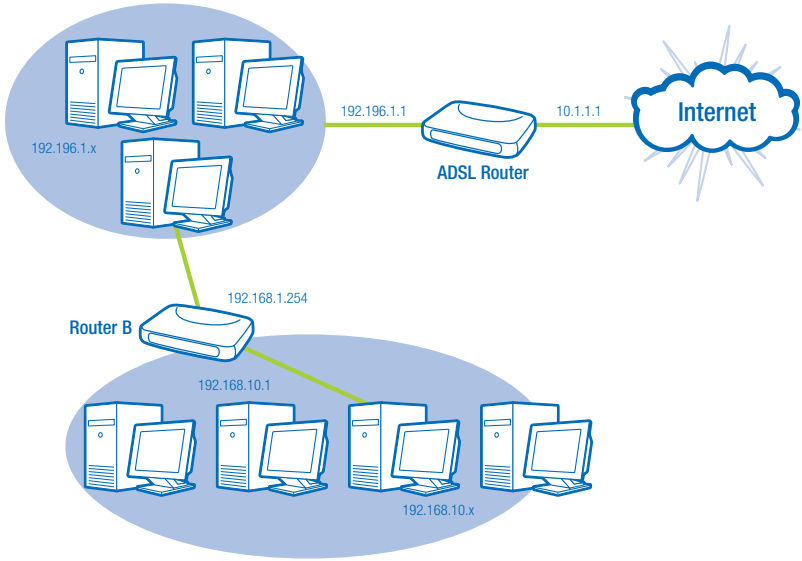


If you don't want the static route that you created, please click the icon in the Delete column from the table.

A dialog window will appear to confirm your action. Click **OK** to remove the static route, or click **Cancel** to keep the setting.

Example – Static Route

Here provides you an example of Static Route.

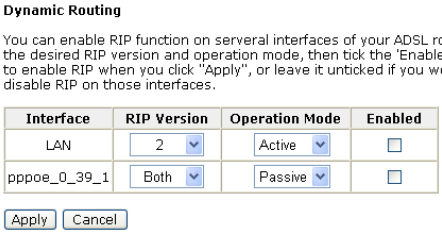


For the LAN shown above, if the PC in the subnet of 192.168.1.x wants to access the PC in the subnet of 192.168.10.x, we can set a static route in the ADSL router, in which the destination is the PC in the subnet 192.168.10.x and the gateway is router B. The setting would be as follows:

Destination: 192.168.10.0
Netmask: 255.255.255.0 (Standard Class C)
Gateway: 192.168.1.254 (Router B)

IP Routing – Dynamic Routing (NB6Plus4W only)

Routing Information Protocol (RIP) is utilized by means of exchanging routing information between routers. It helps the routers to determine optimal routes. This page allows you to enable/disable this function.


Dynamic Routing
You can enable RIP function on serveral interfaces of your ADSL router. Select the desired RIP version and operation mode, then tick the 'Enabled' checkbox to enable RIP when you click "Apply", or leave it unticked if you would like to disable RIP on those interfaces.
Interface
RIP Version
Operation Mode
Enabled
LAN
2
Active
pppoe_0_39_1
Both
Passive
Apply
Cancel

RIP Version:

It incorporates the RIP information when receiving and broadcasting the RIP packets. From the drop down menu, select a RIP version to be accepted, 1, 2 or both.

Operation:

There are two modes for you to choose, Active and Passive. Select Active for transmitting and receiving data, or select Passive for receiving data only.

Enabled:

Check Enabled to enable the RIP function on different interface. Otherwise, disable this function.

Click Apply to invoke the settings set here.

Virtual Server – Port Forwarding

The Router implements NAT to make your entire local network appear as a single machine to the Internet. The typical situation is that you have local servers for different services and you want to make them publicly accessible. With NAT applied, it will translate the internal IP addresses of these servers to a single IP address that is unique on the Internet. NAT function not only eliminates the need for multiple public IP addresses but also provides a measure of security for your LAN.

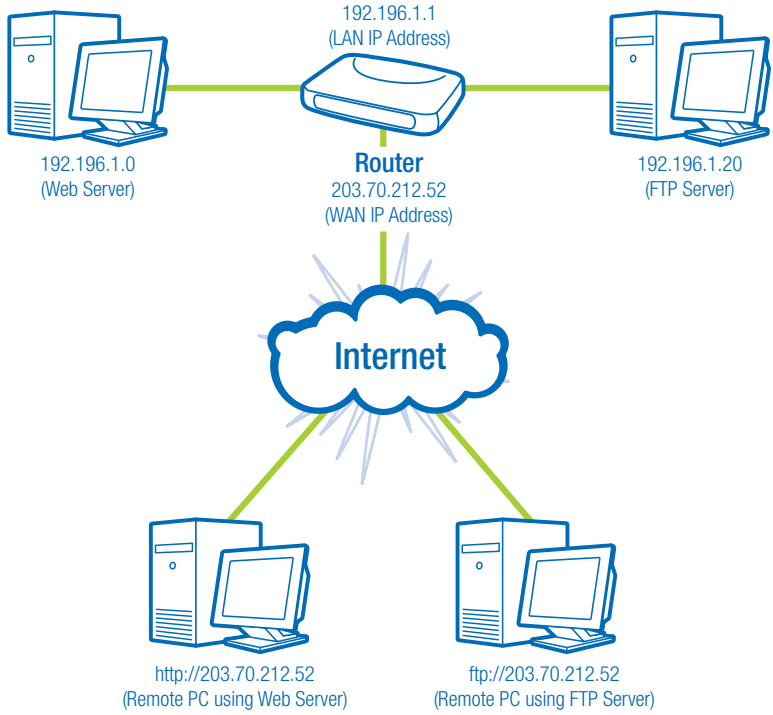
When the router receives an incoming IP packet requesting for accessing your local server, the router will recognize the service type according to the port number in this packet (e.g., port 80 indicates HTTP service and port 21 indicates FTP service). By specifying the port number, the router knows which service should be forwarded to the local IP address that you specified.

After setting the virtual server, you should modify the filter rule about the port and service information which you set on the virtual server. Because the firewall protects the router by filter rule, you should update the filter rule after you set up the virtual server.

Virtual Server function allows you to make servers on your LAN accessible to Internet users. Normally, Internet users would not be able to access a server on your LAN because:

- Your server does not have a valid external IP Address.
- Attempts to connect to devices on your LAN are blocked by the firewall in this device.

The Virtual Server feature solves these problems and allows Internet users to connect to your servers, as illustrated below:



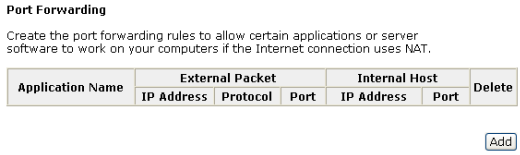
IP Address seen by Internet Users

Once configured, anyone on the Internet can connect to your Virtual Servers.

Please note that, in the above picture, both Internet users are connecting to the same IP address, but using different protocols, such as Http://203.70.212.52 and Ftp://203.70.212.52.

To Internet users, all virtual servers on your LAN have the same IP Address. This IP Address is allocated by your ISP. This address should be static, rather than dynamic, to make it easier for Internet users to connect to your Servers. However, you can use Dynamic DNS feature to allow users to connect to your virtual servers by using a URL, instead of an IP address.

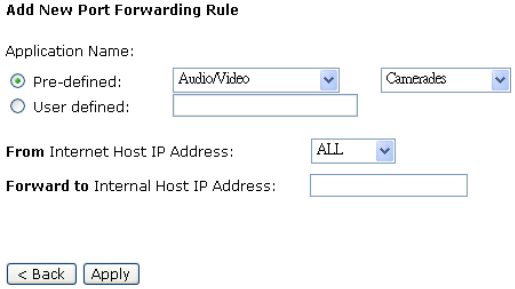
IP addresses can be automatically redirected to local servers configured with private IP addresses. In other words, depending on the requested service (TCP/UDP port number), the router redirects the external service request to the appropriate server (located at another internal IP address).



Add New Port Forwarding

To set a virtual server, please open the **Virtual Server** item from the **Advanced** setup menu.

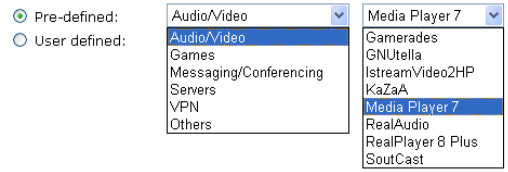
To add a new Port Forwarding, please click **Add** from the **Port Forwarding** web page.

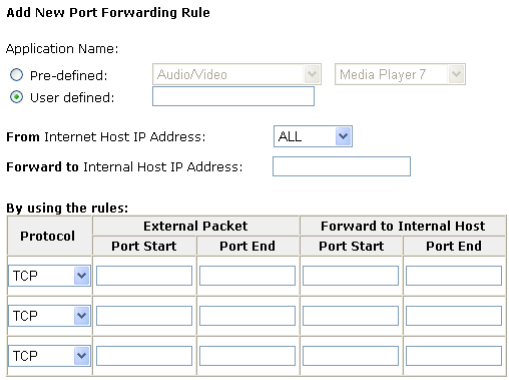


Pre-defined:

Choose one of the service types from the first drop-down list, such as Audio/Video, Games, and so on. In the second drop-down list, choose the name of the application that you want to use with the type that you select in the first list.

For example, if you choose Audio/Video in the first field, the corresponding contents of the second field would be like the drop-down list shown as the following figure.

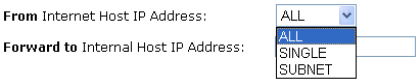




User defined:

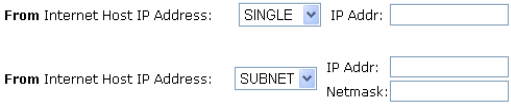
Type a new service name for building a customized service for specific purpose.

There are three lines that you can enter settings into on this page. If you need more lines, just apply the settings and then add a new port forwarding rule.



From Internet Host IP Address:

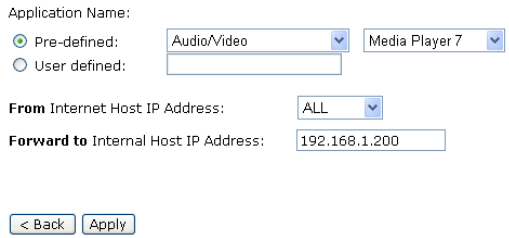
Select the initial place for port forwarding. If you choose **SINGLE**, a box will appear for you to fill in the IP address for the specific host. And, if you choose **SUBNET**, the boxes for IP address and Netmask will appear for you to fill in the IP address and subnet mask for the specific subnet.



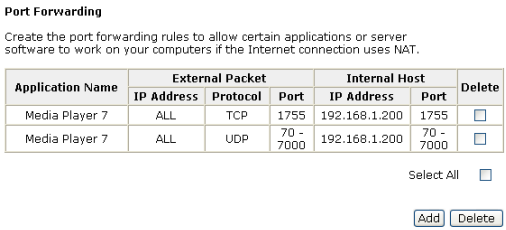
Forward to Internal Host IP Address:

Key in the address for the host used as the destination that information will be forwarded to.

For example, select the predefined application name Audio/Video – Media Player 7, set from ALL internet host IP addresses, and forward to 192.168.1.200. Click **Apply**. Be sure to reboot your router for these changes to take effect.



The result will be displayed as the following figure.



Port Forwarding

Create the port forwarding rules to allow certain applications or server software to work on your computers if the Internet connection uses NAT.

Application Name	External Packet			Internal Host		Delete
	IP Address	Protocol	Port	IP Address	Port	
Media Player 7	ALL	TCP	1755	192.168.1.200	1755	☐
Media Player 7	ALL	UDP	70 - 7000	192.168.1.200	70 - 7000	☐

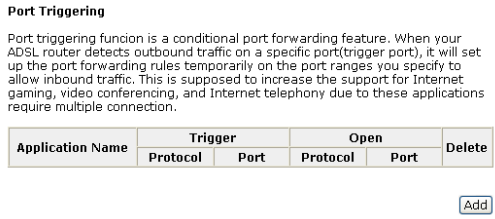
Select All ☐

Add Delete

If you do not want the server that you created, check the **Delete** box of that application and click the **Delete** button to discard it.

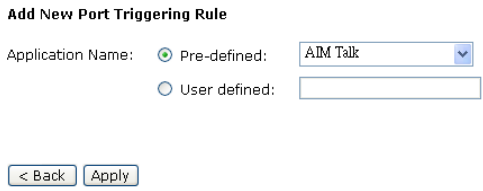
Or if you want to add another one, click **Add** to add a new one.

Virtual Server – Port Triggering

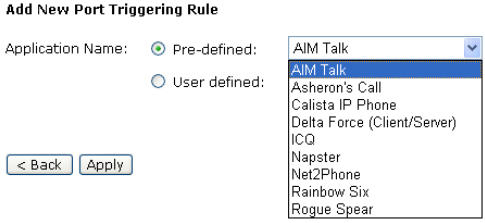

Port Triggering
Port triggering funcion is a conditional port forwarding feature. When your ADSL router detects outbound traffic on a specific port(trigger port), it will set up the port forwarding rules temporarily on the port ranges you specify to allow inbound traffic. This is supposed to increase the support for Internet gaming, video conferencing, and Internet telephony due to these applications require multiple connection.
Application Name
Trigger
Protocol
Port
Open
Protocol
Port
Delete
Add

When the router detects outbound traffic on a specific port, it will set up the port forwarding rules temporarily on the port ranges that you specify to allow inbound traffic. It is supposed to increase the support for Internet gaming, video conferencing, and Internet telephony due to the applications require multiple connection.

To add a new port triggering rule, click **Add** to open this web page. Then choose an application name from the **Pre-defined** list box.



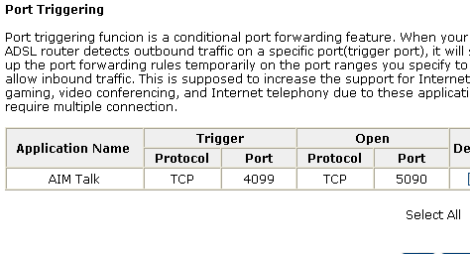
The system provides 9 items for you to choose.



Or define by yourself by typing the name into the field of User defined.

Click Apply to complete the setting.

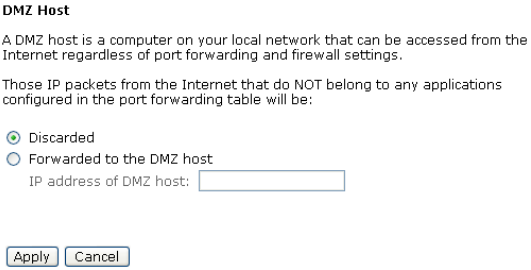
If you select AIM Talk, the result page will be like the demo figure below.


Port Triggering
Port triggering funcion is a conditional port forwarding feature. When your
ADSL router detects outbound traffic on a specific port(trigger port), it will
up the port forwarding rules temporarily on the port ranges you specify to
allow inbound traffic. This is supposed to increase the support for Internet
gaming, video conferencing, and Internet telephony due to these applicati
require multiple connection.
Application Name
Trigger
Protocol
Port
Open
Protocol
Port
AIM Talk
TCP
4099
TCP
5090
Select All

You may delete the application by checking the delete box and pressing Delete.

Virtual Server – DMZ Host

In computer networks, a DMZ (demilitarized zone) is a computer host or small network inserted as a "neutral zone" between a company's private network and the outside public network. It prevents outside users from getting direct access to a server that has company data. A DMZ is an optional and more secure approach to a firewall and effectively acts as a proxy server as well.


DMZ Host
A DMZ host is a computer on your local network that can be accessed from the Internet regardless of port forwarding and firewall settings.
Those IP packets from the Internet that do NOT belong to any applications configured in the port forwarding table will be:
Discarded
Forwarded to the DMZ host
IP address of DMZ host:
Apply
Cancel

To close the function of DMZ Host, please click **Discarded**.

To activate a DMZ host, please click **Forwarded to the DMZ host** radio button, and enter the IP Address of DMZ host.

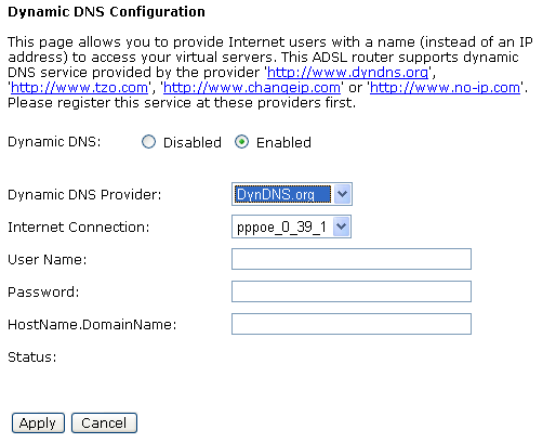
Click **Apply**.

Once this feature is enabled, you must specify an IP address. It allows unrestricted 2-way communication between the specified IP address and other Internet users or Servers.

- This allows almost any application to be used on the specified IP address.
- The specified IP address will receive all "Unknown" connections and data.
- The DMZ feature only works when the NAT function is enabled.

Virtual Server – Dynamic DNS

The Dynamic DNS (Domain Name System) combines both functions of DNS and DHCP to map a dynamic IP to a fixed domain name. This page allows you to access the virtual servers with a domain name and password.


Dynamic DNS Configuration
This page allows you to provide Internet users with a name (instead of an IP address) to access your virtual servers. This ADSL router supports dynamic DNS service provided by the provider 'http://www.dyndns.org', 'http://www.tzo.com', 'http://www.changeip.com' or 'http://www.no-ip.com'. Please register this service at these providers first.
Dynamic DNS: Disabled Enabled
Dynamic DNS Provider: DynDNS.org
Internet Connection: pppoe_0_39_1
User Name:
Password:
HostName.DomainName:
Status:
Apply Cancel

Dynamic DNS:

Select **Enable** to enable DDNS; select **Disabled** to disable this function.

Dynamic DNS Provider:

Choose a provider (DynDNS.org, TZO.com, ChangeIP.com, or No-IP.com) from the drop-down list.

Internet Connection:

Select the interface from the drop-down list that you want to use for connecting the Internet.

User Name / Password:

Enter the user name and password that you registered with the provider.

HostName.DomainName:

Key in the domain name or host name that you registered. You can use letters and dash for naming, yet other characters are not allowed to use for preventing from making troubles.

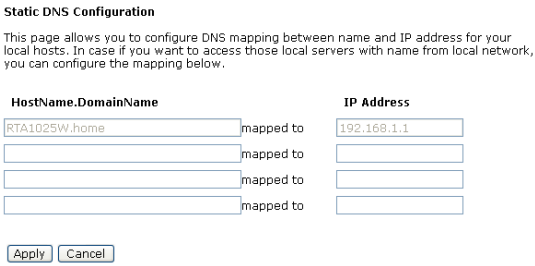
Status:

It displays current status.

When the setting is finished, click **Apply** to invoke them, or click **Cancel** if you want to discard the settings.

Virtual Server – Static DNS

This page allows you to configure DNS mapping between Domain name and IP address for your local hosts. In case you want to access the local servers with domain names from the local network, you can configure the mapping information on the page.


Static DNS Configuration
This page allows you to configure DNS mapping between name and IP address for your local hosts. In case if you want to access those local servers with name from local network, you can configure the mapping below.
HostName.DomainName
IP Address
RTA1025W.home
mapped to
192.168.1.1
mapped to
mapped to
mapped to
Apply
Cancel

Domain Name:

Key in the domain name that you registered at the provider. You can use letters and dash for naming, yet other characters are not allowed to use for preventing from making troubles.

IP Address:

Key in the IP address for the domain name to map.

Click **Apply** to upload your setting.

Firewall

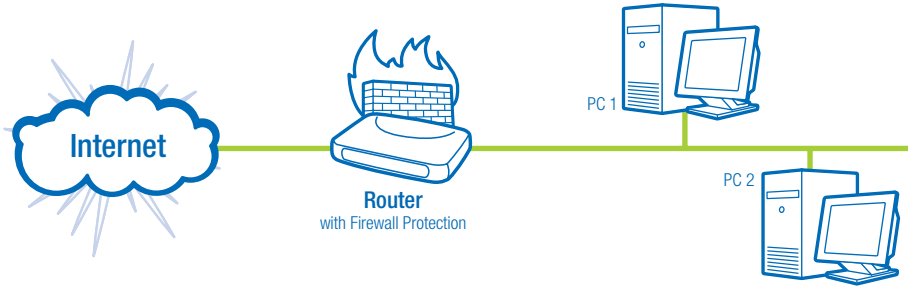
The firewall is a kind of software that interrupts the data between the Internet and your computer. It is the TCP/IP equivalent of a security gate at the entrance to your company. All data must pass through it, and the firewall (functions as a security guard) will allow only authorized data to be passed into the LAN.

What the firewall can do? It can:

- deny or permit any packet from passing through explicitly
- distinguish between various interfaces and match on the following fields:
  - source and destination IP address
  - port

To keep track of the performance of IP Filter, a logging device is used. The device supports logging of the TCP/UDP and IP packet headers and the first 129 bytes of the packet (including headers) whenever a packet is successfully **passed** through or **blocked**, and whenever a packet matches a rule being setup for suspicious packets.

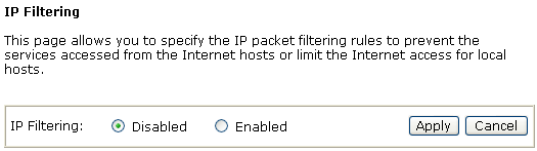
An example for firewall setup:



This picture shows the most common and easiest way to employ the firewall. Basically, you can install a packet-filtering router at the Internet gateway and then configures the filter rule in the router to block or filter protocols and addresses. The systems behind the router usually have a direct access to the Internet; however some dangerous services such as NIS and NFS are usually blocked.

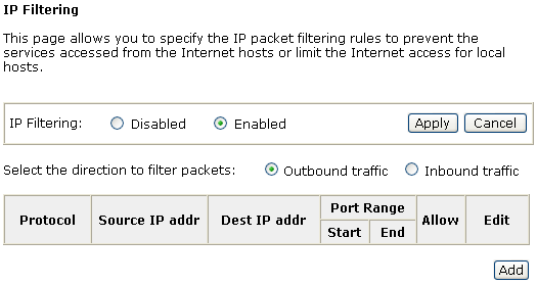
For the security of your router, setting the firewall is an important issue.

Firewall – IP Filtering


IP Filtering
This page allows you to specify the IP packet filtering rules to prevent the services accessed from the Internet hosts or limit the Internet access for local hosts.
IP Filtering: Disabled Enabled Apply Cancel

This page allows you to specify the IP packet filtering rules to prevent the services accessed from the Internet hosts or limit the Internet access for local hosts.

Choose **Disabled** to disable the firewall function. Click **Enabled** to invoke the settings that you set in this web page.

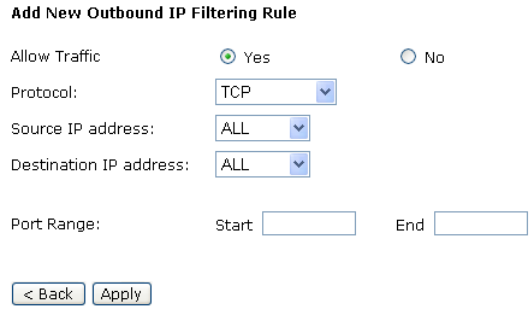

IP Filtering
This page allows you to specify the IP packet filtering rules to prevent the services accessed from the Internet hosts or limit the Internet access for local hosts.
IP Filtering: Disabled Enabled Apply Cancel
Select the direction to filter packets: Outbound traffic Inbound traffic
Protocol
Source IP addr
Dest IP addr
Port Range
Start
End
Allow
Edit
Add

To initiate the IP Filtering, please select the **Enabled** radio button and click **Apply**.

Select the direction to filter packets:

Inbound means the data is transferred from outside onto your computer. Outbound means the data is transferred from your computer onto outside through Internet. Please choose **Outbound traffic** or **Inbound traffic** as the direction for filtering packets.

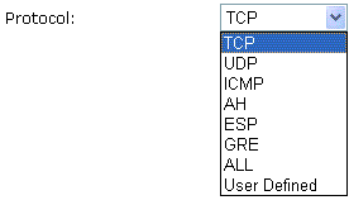
To add a new Filtering rule, click **Add**.



This page provides some settings for you to adjust for adding a new outbound IP Filtering.

Allow Traffic:

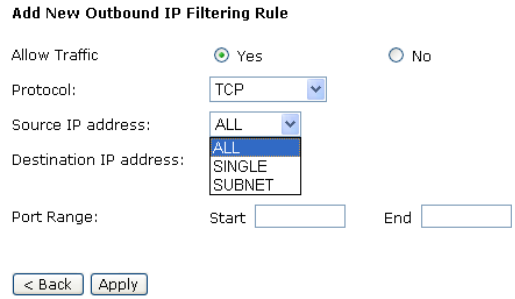
Choose **No** to stop the data transmission, **Yes** to permit the data pass through.



Protocol:

Here provides several default policies for security levels for you to choose. If you don't want to use the predefined setting, you can use **User Defined** to set a customized protocol according to the necessity.

When you choose **User Defined** setting, you have to enter a port number in the "as" field.



Source/Destination IP address:

To specify IP address to allow or deny data transmission, please pull down the drop-down menu to choose a proper one.

The setting **All** means that all the IP addressed in the network are allowed or denied to pass through in Internet.

If you choose **Single**, you will have to key in the specific IP address as the start/end point to let the router identify for granting or denying passing through.

If you choose **Subnet**, you will have to enter the specific IP address and netmask as the start/end point to let the router identify for granting or denying passing through.

Port Range:

The port range is from 0 to 65535. Please key in the start point and end point for the IP Filtering.

After finish the settings, click **Apply**.

Add New Outbound IP Filtering Rule

Allow Traffic: (•) Yes ( ) No

Protocol: TCP

Source IP address: ALL

Destination IP address: ALL

Port Range: Start 0 End 65535

< Back | Apply

Here provides an example shown in the right column. Select TCP as the **Protocol** type, and make the **Source and Destination IP address** to include All, then type 0 and 65535 as the **start and end port**.

IP Filtering

This page allows you to specify the IP packet filtering rules to prevent the services accessed from the Internet hosts or limit the Internet access for local hosts.

IP Filtering: ( ) Disabled (•) Enabled Apply

Select the direction to filter packets: (•) Outbound traffic ( ) Inbound traffic

Protocol	Source IP addr	Dest IP addr	Port Range		Allow	Edit
			Start	End		
TCP	ALL	ALL	0	65535	✓	

Add

A new IP filtering setting for Outbound traffic is created in the web page. To edit the setting, please click to get into the editing page. To delete the setting, click to erase it. To set another IP filtering, click **Add** again.

IP Filtering

This page allows you to specify the IP packet filtering rules to prevent the services accessed from the Internet hosts or limit the Internet access for local hosts.

IP Filtering: ( ) Disabled (•) Enabled Apply

Select the direction to filter packets: ( ) Outbound traffic (•) Inbound traffic

Protocol	Source IP addr	Dest IP addr	Port Range		Allow	Edit
			Start	End		

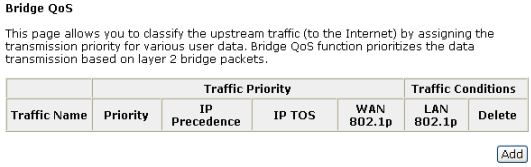
Add

To add a new Inbound IP Filtering, click **Inbound traffic** in the item of **Select the direction to filter packets** on the **IP Filtering** page. Use the same way to add a new one as stated above.

Quality of Service

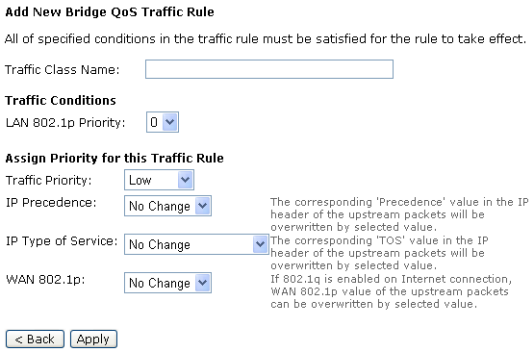
QoS (Quality of Service) is an industry-wide initiative to provide preferential treatment to certain subsets of data, enabling that data to traverse the Internet or intranet with higher quality transmission service.

Quality of Service – Bridge QoS


Bridge QoS
This page allows you to classify the upstream traffic (to the Internet) by assigning the transmission priority for various user data. Bridge QoS function prioritizes the data transmission based on layer 2 bridge packets.
Traffic Priority
Traffic Conditions
Traffic Name
Priority
IP Precedence
IP TOS
WAN 802.1p
LAN 802.1p
Delete
Add

To classify the upstream traffic by assigning the transmission priority for different users' data, please use Bridge QoS to prioritize the data transmission.

The Bridge QoS allows you to set the settings based on layer two bridge packets.

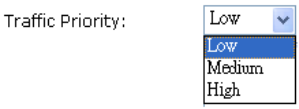

Add New Bridge QoS Traffic Rule
All of specified conditions in the traffic rule must be satisfied for the rule to take effect.
Traffic Class Name:
Traffic Conditions
LAN 802.1p Priority:
0
Assign Priority for this Traffic Rule
Traffic Priority:
Low
IP Precedence:
No Change
The corresponding 'Precedence' value in the IP header of the upstream packets will be overwritten by selected value.
IP Type of Service:
No Change
The corresponding 'TOS' value in the IP header of the upstream packets will be overwritten by selected value.
WAN 802.1p:
No Change
If 802.1q is enabled on Internet connection, WAN 802.1p value of the upstream packets can be overwritten by selected value.
< Back
Apply

Traffic Class Name:

Key in a name as the traffic class for identification.

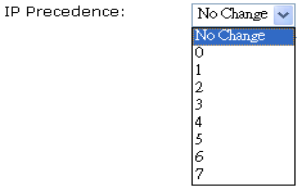
802.1p Priority:

Each incoming packet will be mapped to a specific priority level, so that these levels may be acted on individually to deliver traffic differentiation. Please choose the number (from 0 to 7, low to high priority) for the 802.1p Priority.



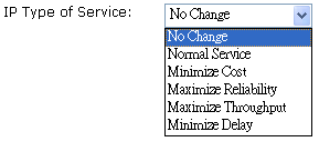
Traffic Priority:

There are three options – Low, Medium, and High that you can choose.



IP Precedence:

The number you choose here decides the type of the IP address processed. No change is the default setting.



IP type of Service:

The system provides some types of service for you to choose. The meaning of each type is the same as the denotation. The default one is No change.

Bridge QoS

This page allows you to classify the upstream traffic (to the Internet) by assigning the transmission priority for various user data. Bridge QoS function prioritizes the data transmission based on layer 2 bridge packets.

	Traffic Priority				Traffic Conditions	
Traffic Name	Priority	IP Precedence	IP TOS	WAN 802.1p	LAN 802.1p	Delete
bridge	Low	No Change	No Change	No Change	0	☐

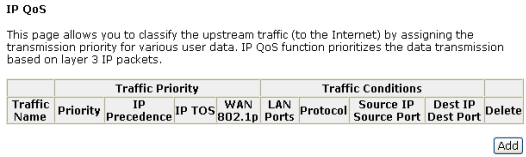
Add Delete

If you set the **LAN 802.1p Priority** 0 as the **traffic condition**, choose **Low traffic priority** for this rule, and set **IP Precedence**, **IP type of service**, and **WAN 802.1p** as no change, after clicking **Apply**, you will get the result as the figure in the right column.

Thus when the users' data matches the traffic condition, the transmission will get a low traffic priority.

You may check the **Delete** box and press **Delete** to discard it, or click **Add** to create more.

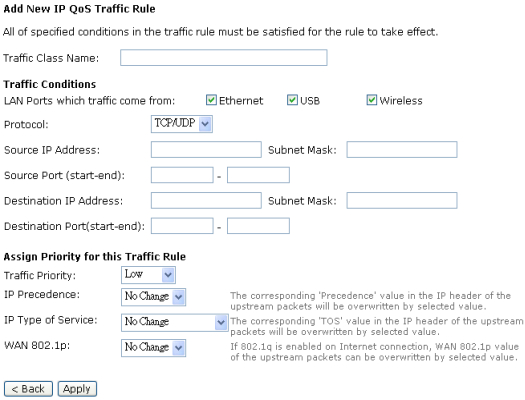
Quality of Service – IP QoS



To classify the upstream traffic by assigning the transmission priority of the data for different users, please use IP QoS to prioritize the data transmission.

The IP QoS allows you to set the settings based on layer three IP packets.

To add a new IP QoS setting, press **Add** in the page of **Quality of Service – IP QoS**, the below page will appear.


Add New IP QoS Traffic Rule
All of specified conditions in the traffic rule must be satisfied for the rule to take effect.
Traffic Class Name:
Traffic Conditions
LAN Ports which traffic come from:
Ethernet
USB
Wireless
Protocol:
TCP/UDP
Source IP Address:
Subnet Mask:
Source Port (start-end):
Destination IP Address:
Subnet Mask:
Destination Port(start-end):
Assign Priority for this Traffic Rule
Traffic Priority:
Low
IP Precedence:
No Change
The corresponding 'Precedence' value in the IP header of the upstream packets will be overwritten by selected value.
IP Type of Service:
No Change
The corresponding 'TOS' value in the IP header of the upstream packets will be overwritten by selected value.
WAN 802.1p:
No Change
If 802.1q is enabled on Internet connection, WAN 802.1p value of the upstream packets can be overwritten by selected value.
< Back
Apply

Traffic Class Name:

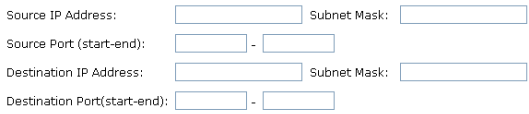
Type a name as the traffic class for identification.

LAN Ports which traffic come from:

The IP QoS rules will be applied on the LAN ports you checked here. The default setting includes all interfaces.

Protocol:

Choose a proper interface for this function. If you don't know how to select, simply use the default one, TCP/UDP.



Source IP Address/ Subnet Mask/ Port:

Key in the **source IP address** (ex.: 192.168.1.0) and **subnet mask** (ex.: 255.255.255.0) for the application (ex.: FTP, HTTP, and so on) that you want to invoke the QoS traffic rule. You may simply enter the **source port**, ranging from 0 to 65535, as the traffic condition.

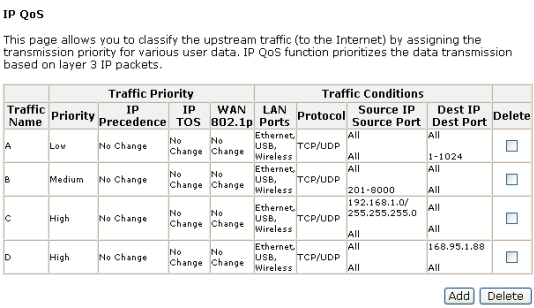
Destination IP/ Subnet Mask/ Port:

Enter the **destination IP address** (ex.: 168.95.1.88) and **subnet mask** (ex.:255.255.255.0) for the application that you want to invoke the QoS traffic rule. Or simply enter the **destination port** for the traffic condition; it ranges from 1 to 65535.

Traffic Priority/ IP Precedence/ IP type of Service/ WAN 802.1p:

Please refer to Bridge QoS.

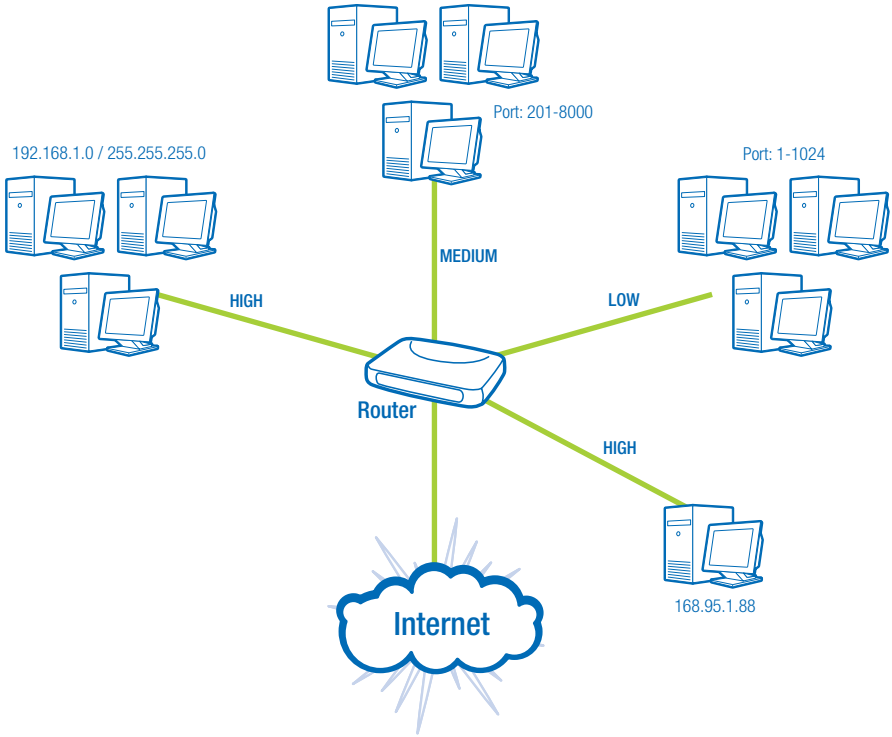
After you click **Apply**, the new QoS setting will be shown below.


IP QoS
This page allows you to classify the upstream traffic (to the Internet) by assigning the transmission priority for various user data. IP QoS function prioritizes the data transmission based on layer 3 IP packets.
Traffic Priority
Traffic Conditions
Traffic Name
Priority
IP Precedence
IP TOS
WAN 802.1p
LAN Ports
Protocol
Source IP Source Port
Dest IP Dest Port
Delete
A Low No Change No Change No Change Ethernet, USB, Wireless TCP/UDP All All All 1-1024
B Medium No Change No Change No Change Ethernet, USB, Wireless TCP/UDP All 201-8000 All All
C High No Change No Change No Change Ethernet, USB, Wireless TCP/UDP 192.168.1.0/ 255.255.255.0 All All All
D High No Change No Change No Change Ethernet, USB, Wireless TCP/UDP All All 168.95.1.88 All
Add
Delete

According to the example, we set four rules for IP QoS. In traffic A, we set 1-1024 as the **destination port**, and the traffic priority is low; in traffic B, the **source port** is from 201 to 8000, and the priority is medium; in traffic C, when the **source IP** is 192.168.1.0, subnet mask is 255.255.255.0, the traffic priority is high; in traffic D, when the traffic is heading to 168.95.1.88, the priority is high.

To delete the rules you set, simply click the check button below **Delete** item and click **Delete** button.

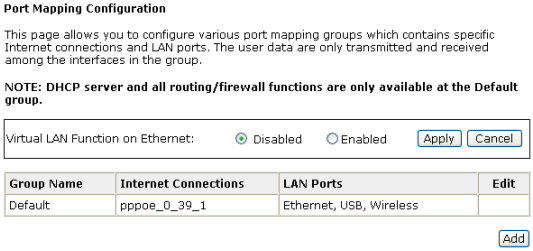
According to our example, the IP QoS configuration can be illustrated by the following figure.



While there are many PCs getting online, the PCs using port 201-8000 to access the internet will have **medium** traffic priority, the PCs carrying 192.168.1.x/ 255.255.255.0 as IP address will have **high** traffic priority. In addition, PCs heading to port 1-1024 will have a **low** priority, while the PCs accessing 168.95.1.88 will have a **high** priority.

Port Mapping

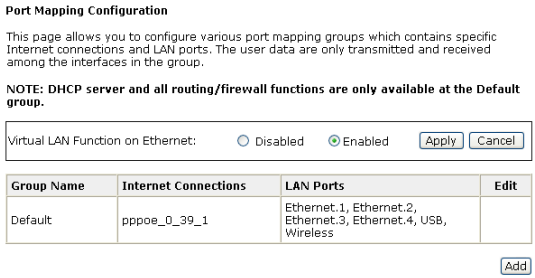
This page allows you to configure various **port mapping groups** which contains specific Internet connections and LAN ports. The user data will be only transmitted and received among the interfaces in the group.


Port Mapping Configuration
This page allows you to configure various port mapping groups which contains specific Internet connections and LAN ports. The user data are only transmitted and received among the interfaces in the group.
NOTE: DHCP server and all routing/firewall functions are only available at the Default group.
Virtual LAN Function on Ethernet:
Disabled
Enabled
Apply
Cancel
Group Name
Internet Connections
LAN Ports
Edit
Default
pppoe_0_39_1
Ethernet, USB, Wireless
Add

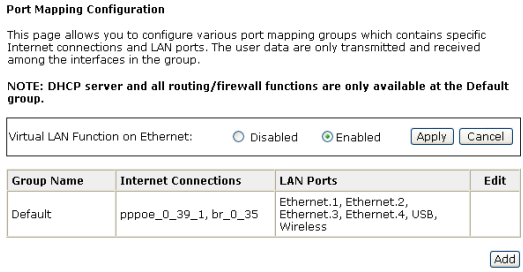
Virtual LAN Function on Ethernet:

If you click **Disabled**, the LAN ports for Ethernet ports will only be shown as an Ethernet interface.

After applying **Enabled**, the LAN ports will be viewed as four separated ports shown on the status chart as below.

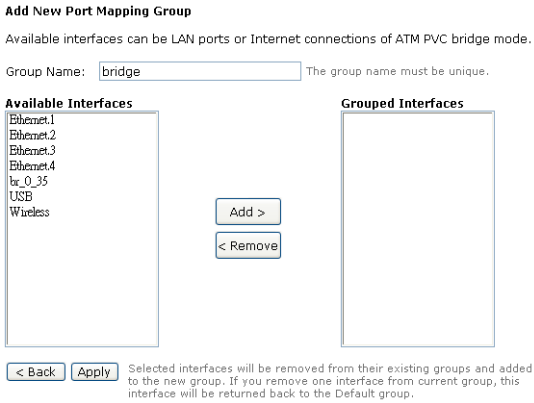

Port Mapping Configuration
This page allows you to configure various port mapping groups which contains specific Internet connections and LAN ports. The user data are only transmitted and received among the interfaces in the group.
NOTE: DHCP server and all routing/firewall functions are only available at the Default group.
Virtual LAN Function on Ethernet:
Disabled
Enabled
Apply
Cancel
Group Name
Internet Connections
LAN Ports
Edit
Default
pppoe_0_39_1
Ethernet.1, Ethernet.2, Ethernet.3, Ethernet.4, USB, Wireless
Add

Normally, this function only needed when more than two PVCs are available, for example, if we have two PVCs, one uses PPPoE and the other uses Bridge mode, we may want to group certain connection to a specific port, especially when some devices may consume higher bandwidth.


Port Mapping Configuration
This page allows you to configure various port mapping groups which contains specific Internet connections and LAN ports. The user data are only transmitted and received among the interfaces in the group.
NOTE: DHCP server and all routing/firewall functions are only available at the Default group.
Virtual LAN Function on Ethernet:
Disabled
Enabled
Apply
Cancel
Group Name
Internet Connections
LAN Ports
Edit
Default
pppoe_0_39_1, br_0_35
Ethernet.1, Ethernet.2, Ethernet.3, Ethernet.4, USB, Wireless
Add

In our following demonstration, we have two PVCs; they are pppoe_0_35_1and br_0_35.

Click **Add** to create a new port mapping group.

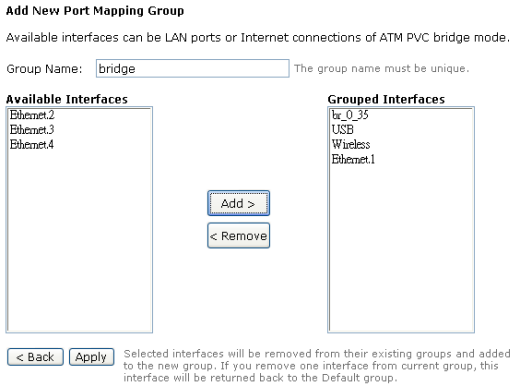

Add New Port Mapping Group
Available interfaces can be LAN ports or Internet connections of ATM PVC bridge mode.
Group Name: bridge
The group name must be unique.
Available Interfaces
Ethernet.1
Ethernet.2
Ethernet.3
Ethernet.4
br_0_35
USB
Wireless
Add >
< Remove
Grouped Interfaces
< Back
Apply
Selected interfaces will be removed from their existing groups and added to the new group. If you remove one interface from current group, this interface will be returned back to the Default group.

Group Name:

Give a unique name here. The word length must not be over the length of the field. In our example, bridge.

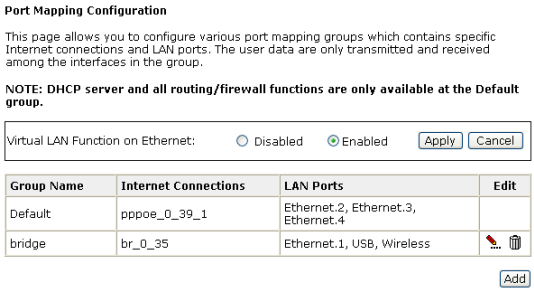
Available Interfaces:

The available interfaces (such as Ethernet, USB, wireless, etc.) will be displayed in the left side box. When you choose it and click **Add**, it will be transferred into the **Grouped Interfaces** at the right side box. Yet, if you want to remove the interface from the current group, it will be returned back to the Default group (left side box) after you click Remove.


Add New Port Mapping Group
Available interfaces can be LAN ports or Internet connections of ATM PVC bridge mode.
Group Name: bridge
The group name must be unique.
Available Interfaces
Ethernet.2
Ethernet.3
Ethernet.4
Add >
< Remove
Grouped Interfaces
br_0_35
USB
Wireless
Ethernet.1
< Back
Apply
Selected interfaces will be removed from their existing groups and added to the new group. If you remove one interface from current group, this interface will be returned back to the Default group.

Now we are going to map USB, Wireless, and the first Ethernet port together with the bridge mode PVC. Click br_0_35 and press Add button, then use the same way to add USB, Wireless, and Ethernet1 to grouped interfaces. The four items are moved to the right box now.

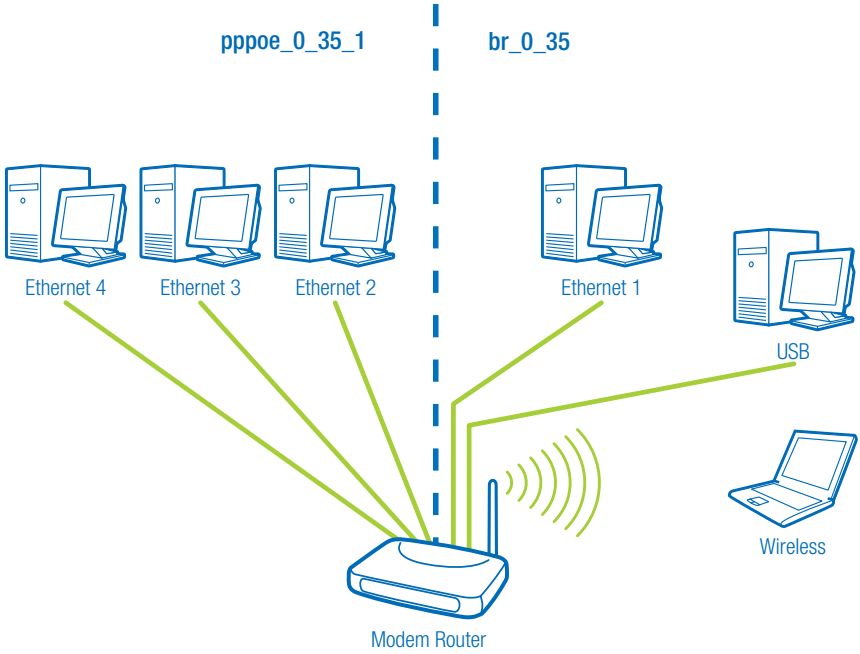
When the setting is done, click **Apply**.


Port Mapping Configuration
This page allows you to configure various port mapping groups which contains specific Internet connections and LAN ports. The user data are only transmitted and received among the interfaces in the group.
NOTE: DHCP server and all routing/firewall functions are only available at the Default group.
Virtual LAN Function on Ethernet:
Disabled
Enabled
Apply
Cancel
Group Name
Internet Connections
LAN Ports
Edit
Default
pppoe_0_39_1
Ethernet.2, Ethernet.3, Ethernet.4
bridge
br_0_35
Ethernet.1, USB, Wireless
Add

Now we can check the result of the port mapping configuration. We have a default group, in which PPPoE mode will be applied through Ethernet port 2, 3, and 4, and we have another group named bridge, in which the bridge mode will be applied on USB, Wireless, and Ethernet port1.

You may click to edit the created group, press to delete it, or click **Add** to create another group.

The following relationship figure illustrates the port mapping configuration.



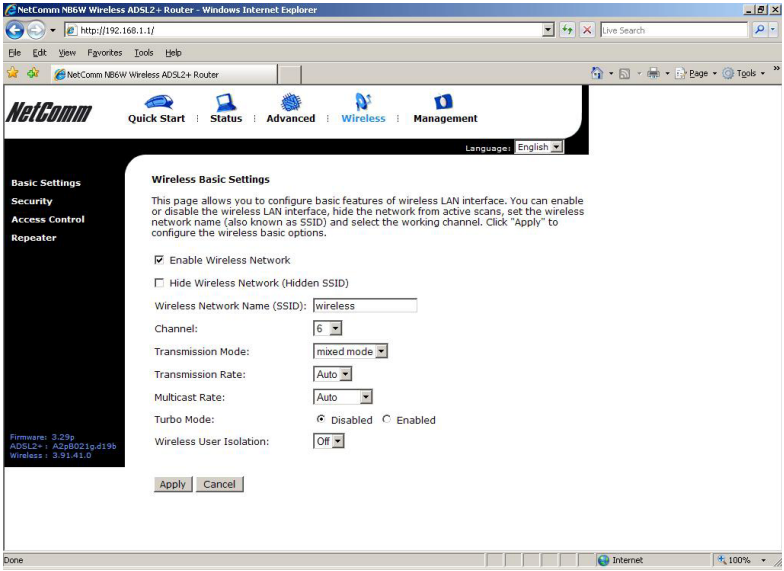
Under this configuration, any devices that is connected to USB, Wireless, or Ethernet port 1 will connect to the internet through the bridge mode PVC **br_0_35**, while the PCs using Ethernet port 2, 3, and 4 will access the internet by the PPPoE connection **pppoe_0_35_1**.

Wireless – NB6W and NB6Plus4W only

This page allows you to configure the router as an Access Point. You may setup the settings for security, access control, and repeater features for this device.

Basic

To set the basic configuration for the wireless features, please open Basic page from the Wireless menu.


NetComm NB6W Wireless ADSL2+ Router - Windows Internet Explorer
http://192.168.1.1/
File Edit View Favorites Tools Help
NetComm NB6W Wireless ADSL2+ Router
NetComm
Quick Start
Status
Advanced
Wireless
Management
Language: English
Basic Settings
Security
Access Control
Repeater
Wireless Basic Settings
This page allows you to configure basic features of wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and select the working channel. Click "Apply" to configure the wireless basic options.
Enable Wireless Network
Hide Wireless Network (Hidden SSID)
Wireless Network Name (SSID): wireless
Channel: 6
Transmission Mode: mixed mode
Transmission Rate: Auto
Multicast Rate: Auto
Turbo Mode: Disabled Enabled
Wireless User Isolation: Off
Apply Cancel
Firmware: 3.29p
ADSL2+ : A2pB021g.d19b
Wireless : 3.91.41.0
Done
Internet
100%

Enable Wireless Network:

Click this check box to enable the wireless network function.

Hide Wireless Network:

Check this box to hide the SSID of this AP (access point). Then other people in the network cannot find the SSID of this device.

Wireless Network Name (SSID):

The system will detect the SSID of your router and displayed in this field for your reference.

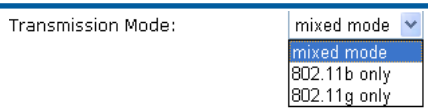
The SSID is the identification characters of a router. The default words will be shown on this page. If you do not check "Hidden SSID" item, the router will periodically broadcasts its SSID to allow the wireless clients within the range to recognize its presence. This can create a security hole since any wireless clients which got the broadcast might associate to your system.

Please note that if you want to communicate, all wireless clients should use the same SSID with the router or access point.

Channel:

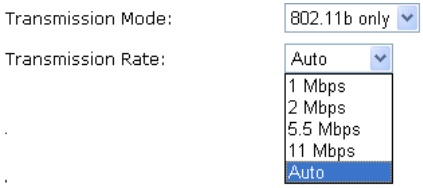
The frequency in which the radio links are about to be established. Select one channel that you want from the drop down list.

As an administrator of network, one must search which channels are available and then assign one available channel as the communication channel. All the other clients that match the SSID and pass security authentication can access this device and will use the same channel that you set here.



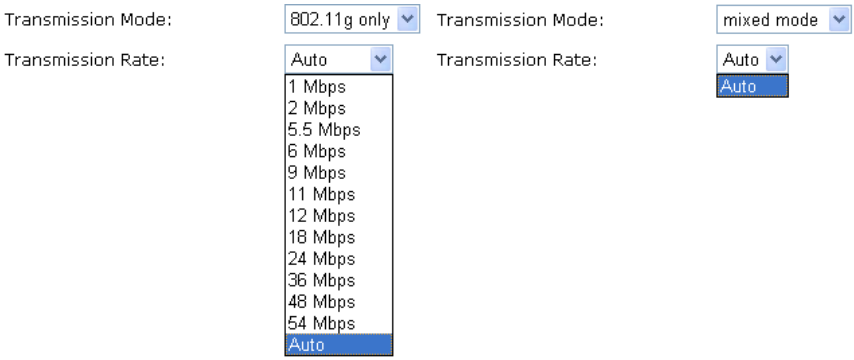
Transmission Mode:

It decides the mode of data transmission. Choose the one that you want to use from the drop-down menu. There are **802.11b only**, **802.11g only** and **Mixed Mode** provided here.



Transmission Rate:

It decides the speed of data transmission. Choose any one of it by using the drop-down menu. This setting will change by the transmission mode that you set above. The transmission rate settings under **802.11b only** include 1, 2, 5.5, 11Mbps and Auto. The transmission rates for **802.11g set**tings include 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54Mbps and Auto. As for **mixed mode**, only Auto is available.



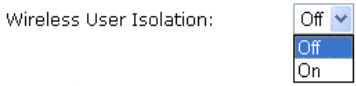
Multicast Rate:

When the multicast transmitting traffics are large, the transmission will be delayed in some way. If you want to speed up the rate, modify from the drop-down list.

For example, you may select 802.11g only as the **transmission mode**, and select high **multicast rate** like 54 Mbps.

Turbo Mode:

When it is enabled, the data transmission will be faster for this router. Check **Enabled** to invoke this function for speeding up the transmission, or check **Disabled** to close this function.



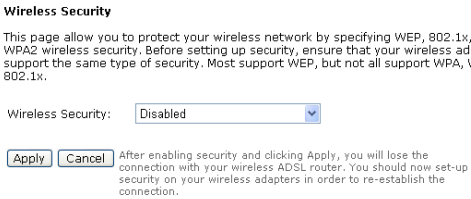
Wireless User Isolation:

To make the communication between the clients, please choose Off. To cut the communication between the clients, please choose On.

Click **Apply** to invoke the settings.

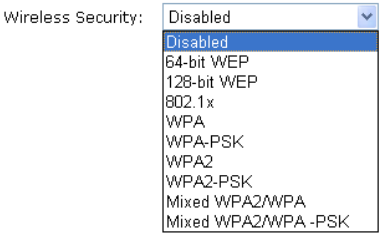
Security

To configure security features for the Wireless interface, please open **Security** item from **Wireless** menu. This web page offers eight authentication protocols for you to secure your data while connecting to networks. There are nine selections including 64-bit and 128-bit WEP, 802.1X, WPA, WPA-PSK, WPA2, WPA2-PSK, mixed WPA2/WPA, and mixed WPA2/WPA-PSK. Different item leads to different web page settings. Please read the following information carefully.


Wireless Security
This page allow you to protect your wireless network by specifying WEP, 802.1x, WPA, or WPA2 wireless security. Before setting up security, ensure that your wireless adaptors support the same type of security. Most support WEP, but not all support WPA, WPA2, or 802.1x.
Wireless Security:
Disabled
Apply
Cancel
After enabling security and clicking Apply, you will lose the connection with your wireless ADSL router. You should now set-up security on your wireless adapters in order to re-establish the connection.

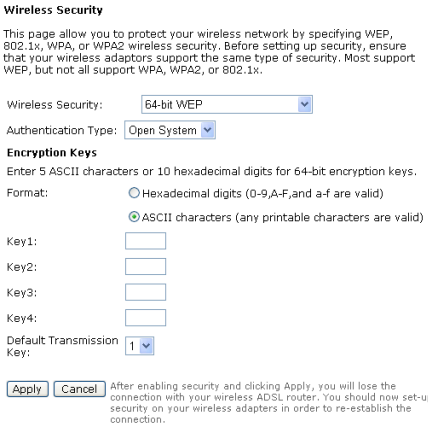
Wireless Security:

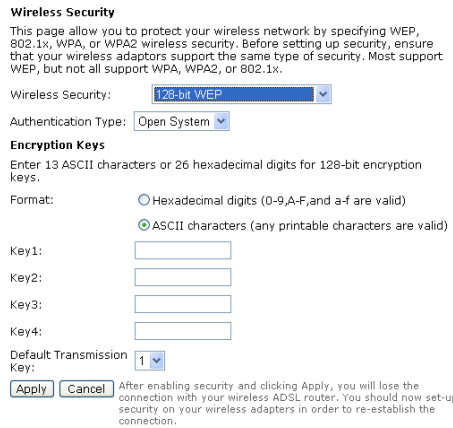
The **Disabled** item offers you the less protection for wireless communication. If you choose **Disabled**, the Encryption Keys will not be shown on this page.



There are nine wireless security modes for you to select.

For 64-bit WEP/128-bit WEP

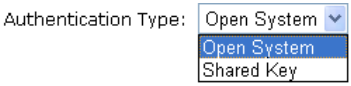

Wireless Security
This page allow you to protect your wireless network by specifying WEP, 802.1x, WPA, or WPA2 wireless security. Before setting up security, ensure that your wireless adaptors support the same type of security. Most support WEP, but not all support WPA, WPA2, or 802.1x.
Wireless Security: 64-bit WEP
Authentication Type: Open System
Encryption Keys
Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys.
Format: Hexadecimal digits (0-9,A-F,and a-f are valid)
ASCII characters (any printable characters are valid)
Key1:
Key2:
Key3:
Key4:
Default Transmission Key: 1
Apply Cancel
After enabling security and clicking Apply, you will lose the connection with your wireless ADSL router. You should now set-up security on your wireless adapters in order to re-establish the connection.


Wireless Security
This page allow you to protect your wireless network by specifying WEP, 802.1x, WPA, or WPA2 wireless security. Before setting up security, ensure that your wireless adaptors support the same type of security. Most support WEP, but not all support WPA, WPA2, or 802.1x.
Wireless Security: 128-bit WEP
Authentication Type: Open System
Encryption Keys
Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys.
Format: Hexadecimal digits (0-9,A-F,and a-f are valid)
ASCII characters (any printable characters are valid)
Key1:
Key2:
Key3:
Key4:
Default Transmission Key: 1
Apply Cancel
After enabling security and clicking Apply, you will lose the connection with your wireless ADSL router. You should now set-up security on your wireless adapters in order to re-establish the connection.

Wireless Security:

By default a minimum level of wireless security has been enabled to help prevent against unwanted wireless users accessing the unit. The default level of wireless security that has been enabled is known as 64 bit Wired Equivalent Privacy or WEP for short. **The default 64 bit Hexadecimal WEP key is: a1b2c3d4e5**

Select the WEP mode for the security function; there are two options, **64-bit** and **128-bit**. Before being transmitted, the data will be encrypted using the encryption key. For example, if you set 64-bit in this field, then the receiving station must be set to use 64 Bit Encryption, and have the same Key value at the same time; otherwise, it will not be able to decrypt the data.

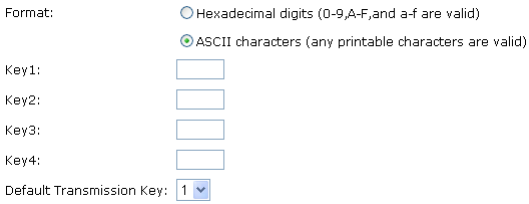


Authentication Type:

The ADSL Router supports two authentication types: **Open System** and **Shared key**. This should be considered with the WEP (Wired Equivalent Privacy) mechanism.

Open System means that it allows any client to authenticate and attempt to communicate with a bridge. The client can only communicate if its WEP keys match the router's WEP keys.

Shared Key means that a bridge or router will send an unencrypted text string to any client attempting to communicate with the router. The client requesting authentication encrypts the text and sends back to the router. Both unencrypted and encrypted can be monitored, yet it leaves the bridge open to be attacked by any intruder if he calculates the WEP key by comparing the text strings. That is why shared key authentication can be less secure than open authentication.



Format:

Choose the form of encryption key. You have to select either **Hexadecimal digits** or **ASCII characters** and type the keys on the fields of Key 1 to Key 4.

Key 1 to 4:

Fill out the WEP keys according to the key length. For **64-bit WEP** mode, the content you can type is 5 characters or 10 hexadecimal digits. For **128-bit WEP** mode, the content you can type is 13 characters or 26 hexadecimal digits.

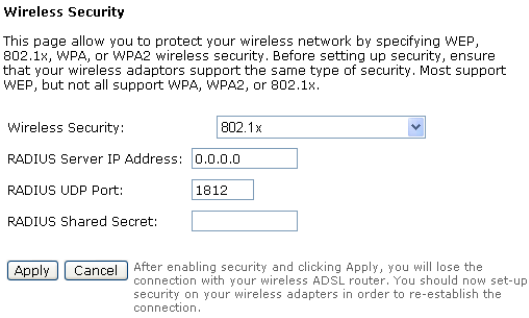
Default Transmission Key:

Select one of the network keys that you set on the Key boxes as the default one.

Click **Apply** for activation when the settings are done.

For 802.1X Wireless Network

When a wireless client requests to access a network, it is required to be authenticated by a central authentication server (RADIUS Server). Only an authenticated user can be granted by the network access and thereby those unauthorized will be blocked.


Wireless Security
This page allow you to protect your wireless network by specifying WEP, 802.1x, WPA, or WPA2 wireless security. Before setting up security, ensure that your wireless adaptors support the same type of security. Most support WEP, but not all support WPA, WPA2, or 802.1x.
Wireless Security:
802.1x
RADIUS Server IP Address:
0.0.0.0
RADIUS UDP Port:
1812
RADIUS Shared Secret:
Apply
Cancel
After enabling security and clicking Apply, you will lose the connection with your wireless ADSL router. You should now set-up security on your wireless adapters in order to re-establish the connection.

Wireless Security:

Choose **802.1x** as the authentication protocol, your data transmission between the router and the clients will be protected with the settings that you set in this web page.

RADIUS Server IP Address:

RADIUS Server is a protocol for carrying authentication, authorization, and configuration information between a Network Access Server which desires to authenticate its links and a shared Authentication Server. Please enter the IP Address for the RADIUS Server.

RADIUS UDP Port:

Port 1812 is the reserved RADIUS- authentication port described in RFC 2138. Earlier AP (RADIUS clients) use port 1945. The default value will be shown on this box. You can keep and use it.

RADIUS Shared Secret:

A shared secret is like a password, which is used between RADIUS Server and the specific AP (RADIUS client) to verify identity. Both RADIUS Server and the AP (RADIUS client) must use the same shared secret for successful communication. Enter the words for the share secret.

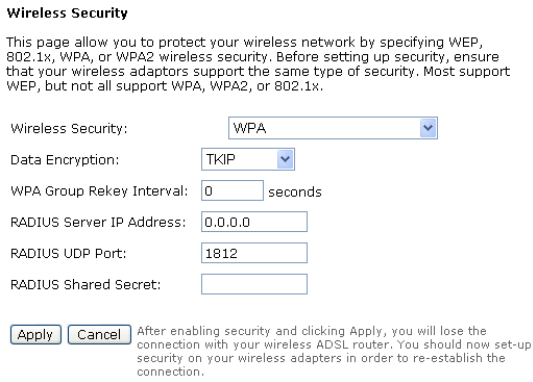
After finishing the settings, click **Apply** for activation.

802.1x environment Configuration

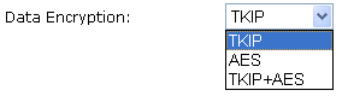
You will need the following components for establishing an 802.1x environment in your network.

- Windows 2000/2003/NT Server: RADIUS server equipped with “Internet Authentication Service”. Certificate Services installed.
- AP (Router): connected to Windows 2000 Advanced Server through the LAN port with DHCP server and 802.1x enabled.
- 802.1x client: a WLAN card supporting WEP.
- Authentication Mechanism.

For WPA (Wi-Fi Protected Access)


Wireless Security
This page allow you to protect your wireless network by specifying WEP, 802.1x, WPA, or WPA2 wireless security. Before setting up security, ensure that your wireless adaptors support the same type of security. Most support WEP, but not all support WPA, WPA2, or 802.1x.
Wireless Security:
WPA
Data Encryption:
TKIP
WPA Group Rekey Interval:
0
seconds
RADIUS Server IP Address:
0.0.0.0
RADIUS UDP Port:
1812
RADIUS Shared Secret:
Apply
Cancel
After enabling security and clicking Apply, you will lose the connection with your wireless ADSL router. You should now set-up security on your wireless adapters in order to re-establish the connection.

The **WPA (WiFi-Protected Access)** authentication is suitable for enterprises. It must be used in conjunction with an authentication server such as RADIUS to provide centralized access control and management. It can provide stronger encryption and authentication solution than none WPA modes.



Data Encryption:

Select the data encryption method for the WPA mode. There are three types that you can choose, **TKIP**, **AES**, **TKIP+AES**.

TKIP (Temporary Key Integrity Protocol) takes the original master key only as a starting point and derives its encryption keys mathematically from this master key. Then it regularly changes and rotates the encryption keys so that the same encryption key will never be used twice.

AES (Advanced Encryption Standard) provides security between client workstations operating in ad hoc mode. It uses a mathematical ciphering algorithm that employs variable key sizes of 128, 192 or 256 bits.

TKIP+AES combine the features and functions of TKIP and AES.

WPA Group Rekey Interval:

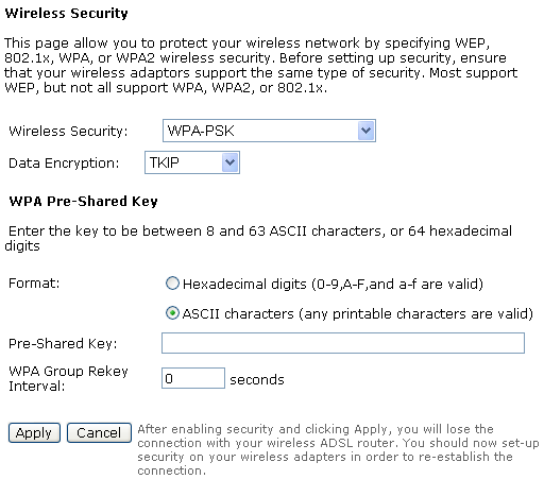
Enter the time for the WPA group rekey interval. The unit is second. With increasing rekey interval, user bandwidth requirement is reduced. On the other hand, the longer the rekey interval, the longer the delay for a new user to gain group access.

RADIUS Server IP Address, RADIUS UDP Port, and RADIUS Shared Secret:

Please refer to the elucidation in the previous **802.1x** section.

After finishing the settings, click **Apply** for activation.

For WPA-PSK; WPA2-PSK; Mixed WPA2/WPA-PSK


Wireless Security
This page allow you to protect your wireless network by specifying WEP, 802.1x, WPA, or WPA2 wireless security. Before setting up security, ensure that your wireless adaptors support the same type of security. Most support WEP, but not all support WPA, WPA2, or 802.1x.
Wireless Security:
WPA-PSK
Data Encryption:
TKIP
WPA Pre-Shared Key
Enter the key to be between 8 and 63 ASCII characters, or 64 hexadecimal digits
Format:
Hexadecimal digits (0-9,A-F,and a-f are valid)
ASCII characters (any printable characters are valid)
Pre-Shared Key:
WPA Group Rekey Interval:
0
seconds
Apply
Cancel
After enabling security and clicking Apply, you will lose the connection with your wireless ADSL router. You should now set-up security on your wireless adapters in order to re-establish the connection.

WPA-PSK (WPA-Pre-Shared Key) is useful for small places without authentication servers such as the network at home. It allows the use of manually-entered keys or passwords and is designed to be easily set up for home users.

Data Encryption:

Select the encryption type for the WPA mode. There are three types that you can choose, TKIP, AES, TKIP+AES. (For more information please refer to WPA section.)

Format:

Choose the form of encryption key. You have to select either Hexadecimal digits or ASCII characters and type the keys on the fields of Pre-Share Key.

Pre-Share Key:

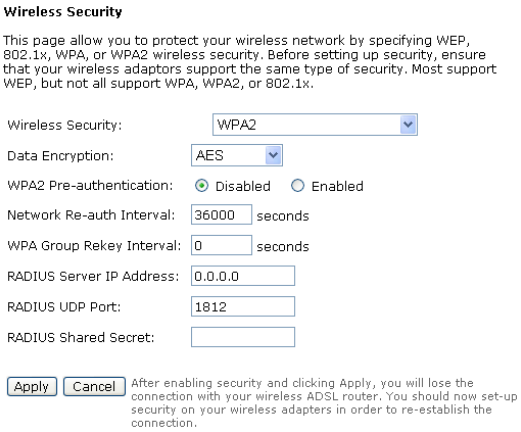
Please enter the key between 8 and 63 characters, or 64 hexadecimal digits. Only the devices with a matching key that you set here can join this network.

WPA Group Rekey Interval:

Enter the time for the WAP group rekey interval. The unit is second. With increasing rekey interval, user bandwidth requirement is reduced.

After finished settings, click Apply for activation.

For WPA-2; Mixed WPA2/WPA


Wireless Security
This page allow you to protect your wireless network by specifying WEP, 802.1x, WPA, or WPA2 wireless security. Before setting up security, ensure that your wireless adaptors support the same type of security. Most support WEP, but not all support WPA, WPA2, or 802.1x.
Wireless Security:
WPA2
Data Encryption:
AES
WPA2 Pre-authentication:
Disabled
Enabled
Network Re-auth Interval:
36000
seconds
WPA Group Rekey Interval:
0
seconds
RADIUS Server IP Address:
0.0.0.0
RADIUS UDP Port:
1812
RADIUS Shared Secret:
Apply
Cancel
After enabling security and clicking Apply, you will lose the connection with your wireless ADSL router. You should now set-up security on your wireless adapters in order to re-establish the connection.

Wireless Security:

The **WPA2** is suitable for enterprises. It must be used in conjunction with an authentication server such as RADIUS to provide centralized access control and management. It can provide stronger encryption and authentication solution than other WPA mode.

Data Encryption:

Select the encryption type for the WPA2 mode. There are three types that you can choose, **TKIP**, **AES**, **TKIP+AES**. (For detailed information please refer to **WPA** section.)

WPA2 Pre-authentication:

The wireless client that has associated with one AP (router A) can do the authentication with another AP (router B) in advance. If the client roams to AP (B), it can associate with AP (B) quickly. Please click **Enabled** to activate this function.

Network Re-auth Interval:

When a wireless client has associated with the AP for a period of time longer than the setting here, it would be disconnected and the authentication will be executed again. The default value is 36000, you may modify it.

WPA Group Rekey Interval:

Enter the time for the WPA group rekey interval. The unit is second. With increasing rekey interval, user bandwidth requirement is reduced.

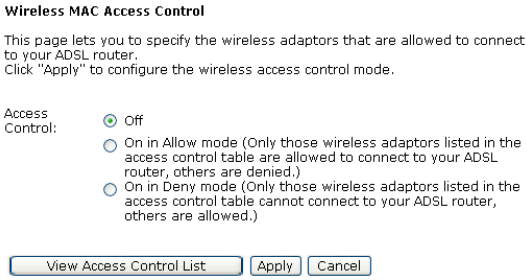
RADIUS Server IP Address, RADIUS UDP Port, and RADIUS Shared Secret:

Please refer to the elucidation in the previous **802.1x** section.

When the settings are finished, click **Apply** for activation.

Access Control

The web page allows you to enable the wireless MAC control configuration.

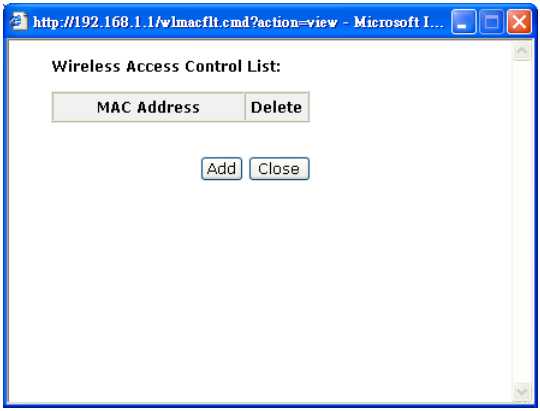

Wireless MAC Access Control
This page lets you to specify the wireless adaptors that are allowed to connect to your ADSL router.
Click "Apply" to configure the wireless access control mode.
Access Control:
Off
On in Allow mode (Only those wireless adaptors listed in the access control table are allowed to connect to your ADSL router, others are denied.)
On in Deny mode (Only those wireless adaptors listed in the access control table cannot connect to your ADSL router, others are allowed.)
View Access Control List
Apply
Cancel

Access Control:

Click Off to disable this function. Click **On in Allow mode** to allow the devices using matched MAC address to link to the AP. And click **On in Deny mode** to disturb the listed wireless MAC address to access the AP.

View Access Control List:

Click this button to view the wireless access control list and to add a new MAC address.

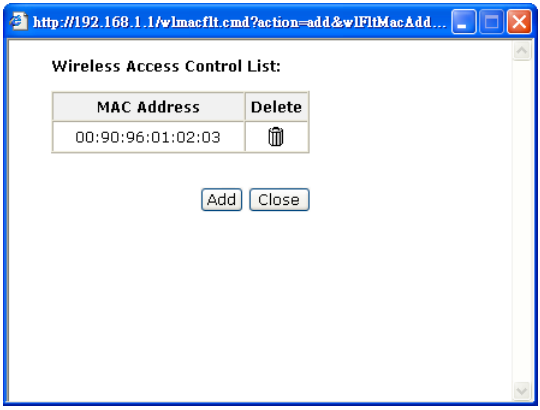


The Wireless Access Control List dialog allows you to add a new MAC address and view current MAC addresses that you had added.

To add a new MAC address to your wireless MAC address filter, click on the **Add** button.

MAC Address of Wireless adaptor:

Key in the MAC Address to be filtered. And click **Apply**.

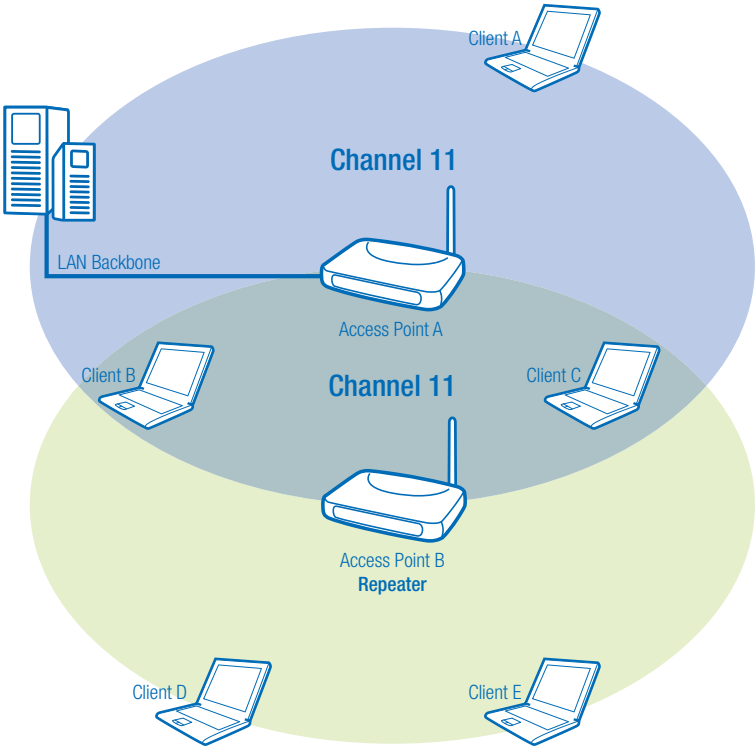


The result of the added MAC address will be shown on the table.

If you want to delete the added MAC address, simply click the delete button, a dialog box will be prompted to confirm the deleting. Click **Yes**, and then the selected one will be erased.

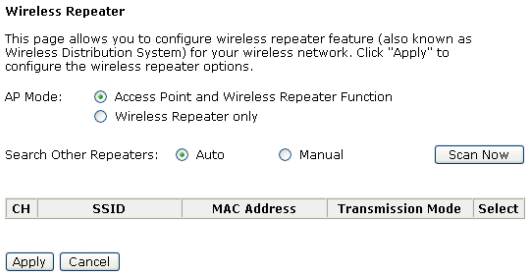
Repeater

A **repeater** is an electronic device that receives a weak or low-level signal and retransmits it at a higher level or higher power, so that the signal can cover longer distances without degradation.



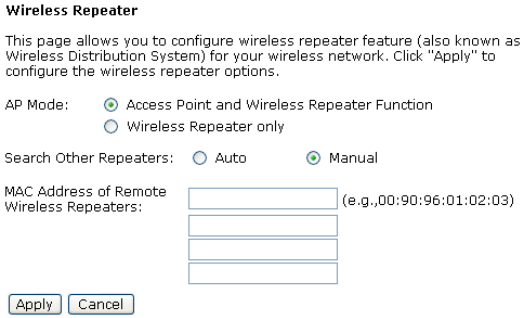
The example figure illustrates the relationship among the AP, the repeater, and the clients. In this example, client A, B, and C can access AP-A, but client D and E cannot. In this case, AP-B works as the repeater for AP-A, and thus client D and E may receive the signal smoothly.

The web page allows you to configure the wireless distribution system for the wireless network.



AP Mode:

Choose an AP mode that you would like to use.


Wireless Repeater
This page allows you to configure wireless repeater feature (also known as Wireless Distribution System) for your wireless network. Click "Apply" to configure the wireless repeater options.
AP Mode:
Access Point and Wireless Repeater Function
Wireless Repeater only
Search Other Repeaters:
Auto
Manual
MAC Address of Remote Wireless Repeaters:
(e.g.,00:90:96:01:02:03)
Apply
Cancel

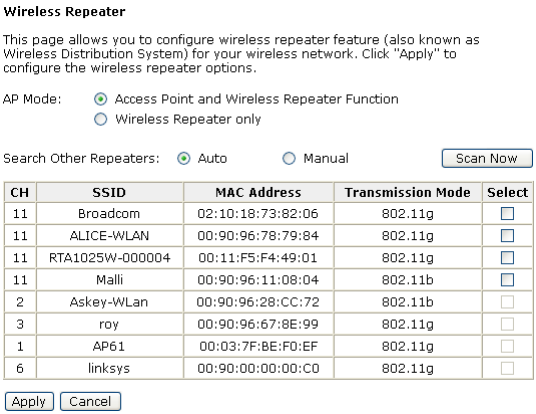
Search Other Repeaters:

You can configure other routers as your repeater by setting up repeater feature mutually. Click the **Scan Now** button to search other repeater in the wireless network automatically. The result will be shown on the chart.

Note: To configure the repeater function among routers, they must use the same SSID and WEP key, so that they may work as repeater for each other.

If you select **Manual** for **Search Other Repeaters**, you will need to type the MAC address for wireless repeaters in the boxes of **MAC Address of Remote Wireless Repeaters**.

The below screen shows an example of executing the function of auto-searching repeaters.


Wireless Repeater
This page allows you to configure wireless repeater feature (also known as Wireless Distribution System) for your wireless network. Click "Apply" to configure the wireless repeater options.
AP Mode:
Access Point and Wireless Repeater Function
Wireless Repeater only
Search Other Repeaters:
Auto
Manual
Scan Now
CH SSID MAC Address Transmission Mode Select
11 Broadcom 02:10:18:73:82:06 802.11g
11 ALICE-WLAN 00:90:96:78:79:84 802.11g
11 RTA1025W-000004 00:11:F5:F4:49:01 802.11g
11 Malli 00:90:96:11:08:04 802.11b
2 Askey-WLan 00:90:96:28:CC:72 802.11b
3 roy 00:90:96:67:8E:99 802.11g
1 AP61 00:03:7F:BE:F0:EF 802.11g
6 linksys 00:90:00:00:00:C0 802.11g
Apply
Cancel

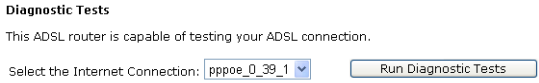
You may select the routers (which use the same channel as yours) from the table and configure the same SSID and WEP key with the one you chose, so that they can function as repeaters to extend the coverage area for each other.

When you finish the settings, please click **Apply** to invoke them.

Management

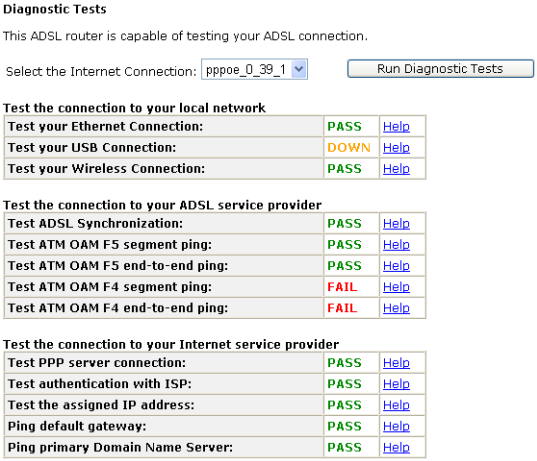
Diagnostics

To check the linking status for the network and your computer, a diagnostic test can guide you to detect the network problem. The testing items are listed and examined one by one. If the previous one is failed, than the items following that one will be failed, too. Use this diagnostic test to detect the connectivity mistakes whenever linking problem occurs.


Diagnostic Tests
This ADSL router is capable of testing your ADSL connection.
Select the Internet Connection: pppoe_0_39_1
Run Diagnostic Tests

Press Run Diagnostic Tests on the Diagnostic Tests page.

The Result would be shown on the same page.

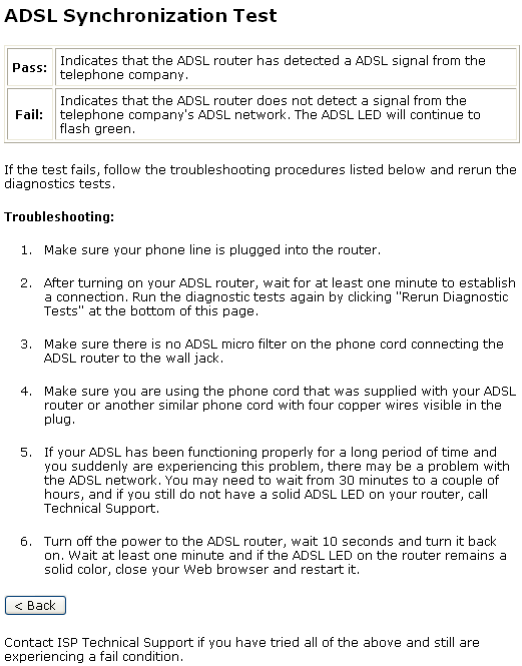

Diagnostic Tests
This ADSL router is capable of testing your ADSL connection.
Select the Internet Connection: pppoe_0_39_1
Run Diagnostic Tests
Test the connection to your local network
Test your Ethernet Connection: PASS Help
Test your USB Connection: DOWN Help
Test your Wireless Connection: PASS Help
Test the connection to your ADSL service provider
Test ADSL Synchronization: PASS Help
Test ATM OAM F5 segment ping: PASS Help
Test ATM OAM F5 end-to-end ping: PASS Help
Test ATM OAM F4 segment ping: FAIL Help
Test ATM OAM F4 end-to-end ping: FAIL Help
Test the connection to your Internet service provider
Test PPP server connection: PASS Help
Test authentication with ISP: PASS Help
Test the assigned IP address: PASS Help
Ping default gateway: PASS Help
Ping primary Domain Name Server: PASS Help

For the item which passes through the diagnostics, a "**PASS**" will be displayed on the right side of that item.

If not, a "**FAIL**" will be presented there.

If there is no device using that port, a "**DOWN**" will be displayed.

Press the **Help** link to know what the result (Pass, Fail) represents for.



ADSL Synchronization Test

Pass:	Indicates that the ADSL router has detected a ADSL signal from the telephone company.
Fail:	Indicates that the ADSL router does not detect a signal from the telephone company's ADSL network. The ADSL LED will continue to flash green.

If the test fails, follow the troubleshooting procedures listed below and rerun the diagnostics tests.

Troubleshooting:

1. Make sure your phone line is plugged into the router.
2. After turning on your ADSL router, wait for at least one minute to establish a connection. Run the diagnostic tests again by clicking "Rerun Diagnostic Tests" at the bottom of this page.
3. Make sure there is no ADSL micro filter on the phone cord connecting the ADSL router to the wall jack.
4. Make sure you are using the phone cord that was supplied with your ADSL router or another similar phone cord with four copper wires visible in the plug.
5. If your ADSL has been functioning properly for a long period of time and you suddenly are experiencing this problem, there may be a problem with the ADSL network. You may need to wait from 30 minutes to a couple of hours, and if you still do not have a solid ADSL LED on your router, call Technical Support.
6. Turn off the power to the ADSL router, wait 10 seconds and turn it back on. Wait at least one minute and if the ADSL LED on the router remains a solid color, close your Web browser and restart it.

< Back

Contact ISP Technical Support if you have tried all of the above and still are experiencing a fail condition.

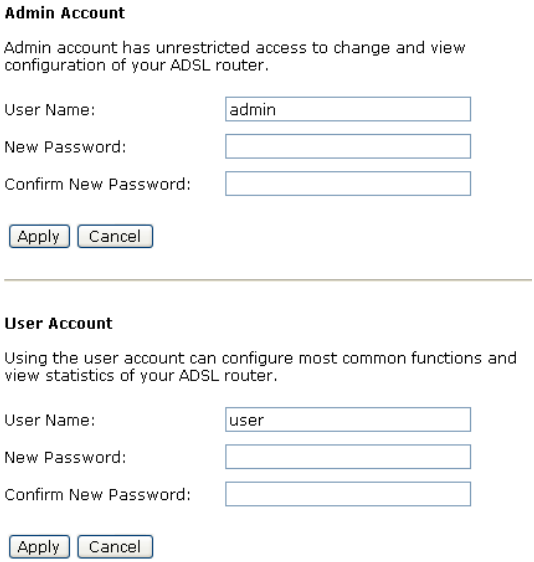
Take the Help link of ADSL Synchronization for example.

It not only explains the situation for Pass and Fail, but offers the troubleshooting procedures for you to follow.

Press **Back** to return.

Management Accounts

This page allows you to CHANGE the user name and password for accessing your ADSL Router.



For the **Admin Account**, the default setting for both username and password are **admin**. If you want to change the username and the password, please modify the **User Name** and **New Password**, and then retype the new password in the **Confirm** field for confirmation. Then click **Apply**.

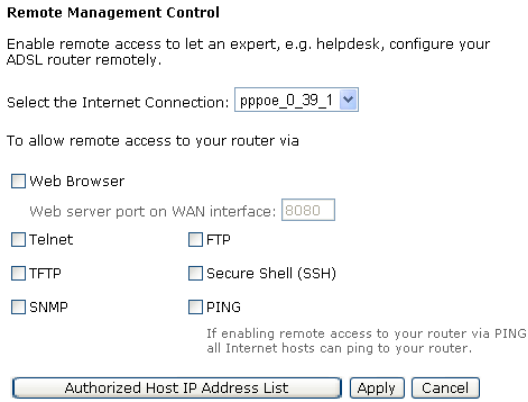
To create a user account, you may setup a username and password under **User Account** on the same page.

Note that the new user can merely access the **Quick Start** and **Status** page.

Management Control – From Remote

There are various interfaces for the remote access. Please choose from them if you want to enable the remote access control.

Note: NB6 supports Web Browser, Telnet, TFTP and Ping only


Remote Management Control
Enable remote access to let an expert, e.g. helpdesk, configure your ADSL router remotely.
Select the Internet Connection: pppoe_0_39_1
To allow remote access to your router via
Web Browser
Web server port on WAN interface: 8080
Telnet
FTP
TFTP
Secure Shell (SSH)
SNMP
PING
If enabling remote access to your router via PING, all Internet hosts can ping to your router.
Authorized Host IP Address List
Apply
Cancel

Select the Internet Connect:

Select one connection item from the drop-down list to enable the function.

Web Browser:

Check this box if you want to have remote control through HTTP. The default port number is 8080. Modify the port whenever you want.

Telnet:

Check this box if you want to have remote control through telnet.

FTP:

Choose this box if you want to have remote control through FTP.

TFTP:

Choose this box if you want to have remote control through TFTP.

Secure Shell (SSH):

Choose this box if you want to have remote control through SSH.

SNMP:

Choose this box if you want to have remote control through SNMP agent.

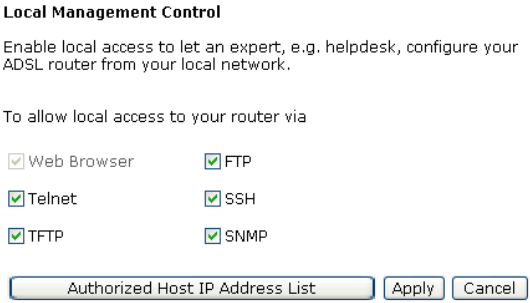
Ping:

Choose this box if you want to have remote control through ping command under DOS prompt.

Authorized Host IP Address List:

Decide whether all internet hosts can access your IAD or only authorized internet hosts can access. Click **Apply** to save your setting.

Management Control – From Local



You can allow local access to your router via the checked interfaces.

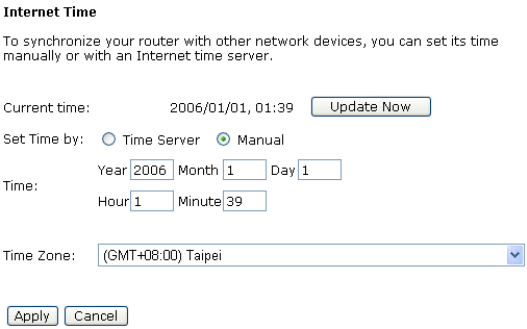
Note: NB6 supports Web Browser, Telnet, TFTP and Ping only

Authorized Host IP Address List:

Refer to Remote Management Control.

Click **Apply** to activate your settings or click **Cancel** to retain the original settings.

Internet Time


Internet Time
To synchronize your router with other network devices, you can set its time manually or with an Internet time server.
Current time: 2006/01/01, 01:39 Update Now
Set Time by: Time Server Manual
Time: Year 2006 Month 1 Day 1
Hour 1 Minute 39
Time Zone: (GMT+08:00) Taipei
Apply Cancel

The router's clock must synchronize with global Internet time. The time you set in the screen will be adapted to system log.

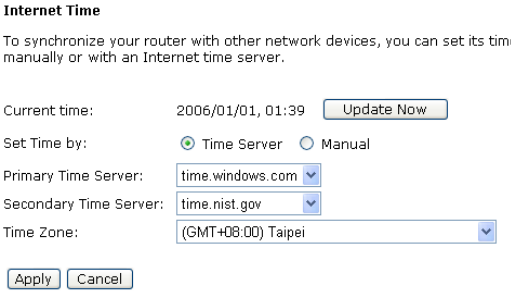
Update Now:

Click this button to refresh the current time.

Set Time by (Time Server/ Manual):

The default setting is Manual. Select this one, and set the start time by typing the date and the time manually to help the router perform tasks.

If you select Time Server, the system will set time via time server automatically.


Internet Time
To synchronize your router with other network devices, you can set its time manually or with an Internet time server.
Current time: 2006/01/01, 01:39 Update Now
Set Time by: Time Server Manual
Primary Time Server: time.windows.com
Secondary Time Server: time.nist.gov
Time Zone: (GMT+08:00) Taipei
Apply Cancel

Primary Time Server/ Secondary Time Server:

You may select the preferred time server from the drop-down list. The time will be adjusted by the time server.

Time Zone:

Choose the time zone of your location.

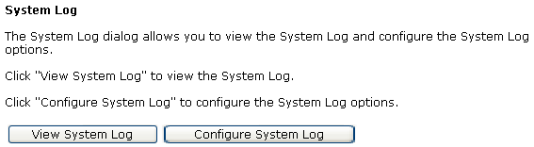
Apply:

Save the data on the screen and apply the data after restarting the router.

Cancel:

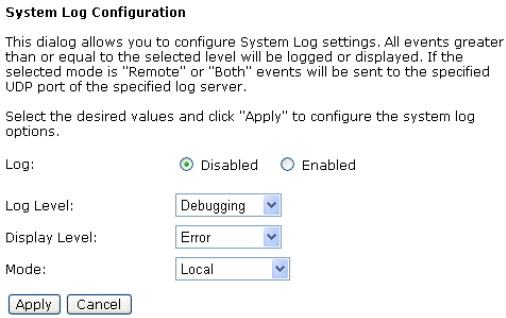
Discard the new configuration and reserve the original settings.

System Log


System Log
The System Log dialog allows you to view the System Log and configure the System Log options.
Click "View System Log" to view the System Log.
Click "Configure System Log" to configure the System Log options.
View System Log
Configure System Log

As shown on the web page, you can view the system log and configure system log whenever you want.

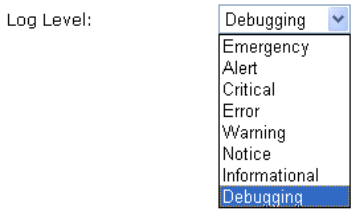
To view the system log, you must configure system log first. Press **Configure System Log** to start.


System Log Configuration
This dialog allows you to configure System Log settings. All events greater than or equal to the selected level will be logged or displayed. If the selected mode is "Remote" or "Both" events will be sent to the specified UDP port of the specified log server.
Select the desired values and click "Apply" to configure the system log options.
Log:
Disabled
Enabled
Log Level:
Debugging
Display Level:
Error
Mode:
Local
Apply
Cancel

Configuring System Log

You can **enable** or **disable** the log function, and choose **log level**, **display level** and proper **mode** as you like. Then click **Apply** to invoke the settings or press **Cancel** to discard them.

There are 8 types of **log level** and **display level** for you to choose.



Log Level:

This function enables you to decide how detailed the messages will be stored. Set a proper level according to your needs. The default Log Level is **Debugging**.

The **Debugging** Level logs all messages to the file, while the **Emergency** Level logs fatal messages only. The lower the item is, the more detailed information it provides; i.e., debugging level stores the most detailed information.

Owing to the limitation of the storage on the ADSL router, the former information will be erased and replaced by the latest message automatically when the buffer is overflowed.

Display Level:

For the convenience of the users, the display level can function as a filter. It decides the level for the messages to exhibit when the user wants to view the logs on the local side. For example, for a programmer or engineer, he/she may want to know about debugging or informational level message;

for general users, they may only need or want to learn about error, critical, alert, or emergency messages only. The default Display Level is **Error**.

Therefore, when the log level is "Debugging" and the display level is "Error", the CPE logs the most detailed message but shows error level data only.

Mode:

You can choose where to store the logs; the options include **Local**, **Remote** and **Both**. Local means the CPE, i.e., the ADSL Router. Remote means the log server you specified to forward the log information to. The default mode is Local.

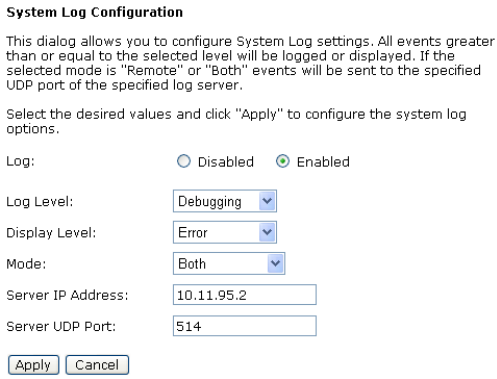
If you choose **Remote** or **Both**, you have to specify the **Server IP Address** and **UDP Port**, and all the events will be sent to the specified UDP port of the specified log server.

Note: Display Level only filters for the local side. All the messages will be displayed on the remote Log Server.

Example

Suppose we are going to record the system logs on both the ADSL Router and the Server bearing IP address 10.11.95.2, the procedures below illustrate the situation:

System Log Configuration


System Log Configuration
This dialog allows you to configure System Log settings. All events greater than or equal to the selected level will be logged or displayed. If the selected mode is "Remote" or "Both" events will be sent to the specified UDP port of the specified log server.
Select the desired values and click "Apply" to configure the system log options.
Log:
Disabled
Enabled
Log Level:
Debugging
Display Level:
Error
Mode:
Both
Server IP Address:
10.11.95.2
Server UDP Port:
514
Apply
Cancel

1. Choose **Enabled** Log.
2. Select Debugging as the **Log Level**, and Error as the **Display Level**. (Or select other level according to your needs.)
3. Set the **Mode** as Both, key in the **Server IP Address** as 10.11.95.2, and leave the **Server UDP Port** as the default value 514.
4. Press **Apply** to invoke the settings.

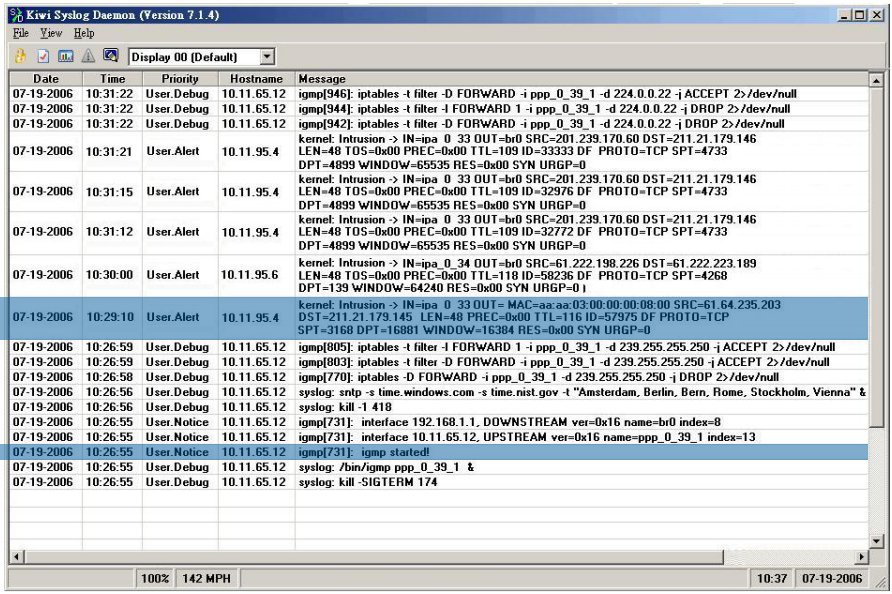
Viewing System Log – Remote Side (Server)

To view the system log on the Log Server (10.11.95.2), a log viewing tool must be installed.

1. Download the Kiwi Syslog Daemon from Kiwi Enterprises. (http://www.kiwisyslog.com/downloads.php)

   Kiwi Syslog Daemon is a freeware Syslog Daemon for Windows. It receives, logs, displays and forwards Syslog messages from hosts such as routers, switches, and any other syslog enabled device. You can choose other logger tools; here, we use Kiwi for example.

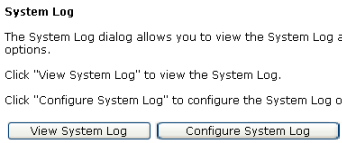
2. Install the Kiwi Syslog server software on the PC (10.11.95.2).
3. Open the **Kiwi Syslog Daemon** application. You will get to a screen shown as follows.


Kiwi Syslog Daemon (Version 7.1.4)
File View Help
Display 00 (Default)
Date Time Priority Hostname Message
07-19-2006 10:31:22 User.Debug 10.11.65.12 igmp[946]: iptables -t filter -D FORWARD -i ppp_0_39_1 -d 224.0.0.22 -j ACCEPT 2>/dev/null
07-19-2006 10:31:22 User.Debug 10.11.65.12 igmp[944]: iptables -t filter -I FORWARD 1 -i ppp_0_39_1 -d 224.0.0.22 -j DROP 2>/dev/null
07-19-2006 10:31:22 User.Debug 10.11.65.12 igmp[942]: iptables -t filter -D FORWARD -i ppp_0_39_1 -d 224.0.0.22 -j DROP 2>/dev/null
07-19-2006 10:31:21 User.Alert 10.11.95.4 kernel: Intrusion -> IN=ipa_0_33 OUT=br0 SRC=201.239.170.60 DST=211.21.179.146 LEN=48 TOS=0x00 PREC=0x00 TTL=109 ID=33333 DF PROTO=TCP SPT=4733 DPT=4899 WINDOW=65535 RES=0x00 SYN URGP=0
07-19-2006 10:31:15 User.Alert 10.11.95.4 kernel: Intrusion -> IN=ipa_0_33 OUT=br0 SRC=201.239.170.60 DST=211.21.179.146 LEN=48 TOS=0x00 PREC=0x00 TTL=109 ID=32976 DF PROTO=TCP SPT=4733 DPT=4899 WINDOW=65535 RES=0x00 SYN URGP=0
07-19-2006 10:31:12 User.Alert 10.11.95.4 kernel: Intrusion -> IN=ipa_0_33 OUT=br0 SRC=201.239.170.60 DST=211.21.179.146 LEN=48 TOS=0x00 PREC=0x00 TTL=109 ID=32772 DF PROTO=TCP SPT=4733 DPT=4899 WINDOW=65535 RES=0x00 SYN URGP=0
07-19-2006 10:30:00 User.Alert 10.11.95.6 kernel: Intrusion -> IN=ipa_0_34 OUT=br0 SRC=61.222.198.226 DST=61.222.223.189 LEN=48 TOS=0x00 PREC=0x00 TTL=118 ID=58236 DF PROTO=TCP SPT=4268 DPT=139 WINDOW=64240 RES=0x00 SYN URGP=0
1
07-19-2006 10:29:10 User.Alert 10.11.95.4 kernel: Intrusion -> IN=ipa_0_33 OUT= MAC=aa:aa:03:00:00:00:08:00 SRC=61.64.235.203 DST=211.21.179.145 LEN=48 PREC=0x00 TTL=116 ID=57975 DF PROTO=TCP SPT=3168 DPT=16881 WINDOW=16384 RES=0x00 SYN URGP=0
07-19-2006 10:26:59 User.Debug 10.11.65.12 igmp[805]: iptables -t filter -I FORWARD 1 -i ppp_0_39_1 -d 239.255.255.250 -j ACCEPT 2>/dev/null
07-19-2006 10:26:59 User.Debug 10.11.65.12 igmp[803]: iptables -t filter -D FORWARD -i ppp_0_39_1 -d 239.255.255.250 -j ACCEPT 2>/dev/null
07-19-2006 10:26:58 User.Debug 10.11.65.12 igmp[770]: iptables -D FORWARD -i ppp_0_39_1 -d 239.255.255.250 -j DROP 2>/dev/null
07-19-2006 10:26:56 User.Debug 10.11.65.12 syslog: sntp -s time.windows.com -s time.nist.gov -t "Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna" &
07-19-2006 10:26:56 User.Debug 10.11.65.12 syslog: kill -1 418
07-19-2006 10:26:55 User.Notice 10.11.65.12 igmp[731]: interface 192.168.1.1, DOWNSTREAM ver=0x16 name=br0 index=8
07-19-2006 10:26:55 User.Notice 10.11.65.12 igmp[731]: interface 10.11.65.12, UPSTREAM ver=0x16 name=ppp_0_39_1 index=13
2
07-19-2006 10:26:55 User.Notice 10.11.65.12 igmp[731]: igmp started!
07-19-2006 10:26:55 User.Debug 10.11.65.12 syslog: /bin/igmp ppp_0_39_1 &
07-19-2006 10:26:55 User.Debug 10.11.65.12 syslog: kill -SIGTERM 174
100% 142 MPH 10:37 07-19-2006

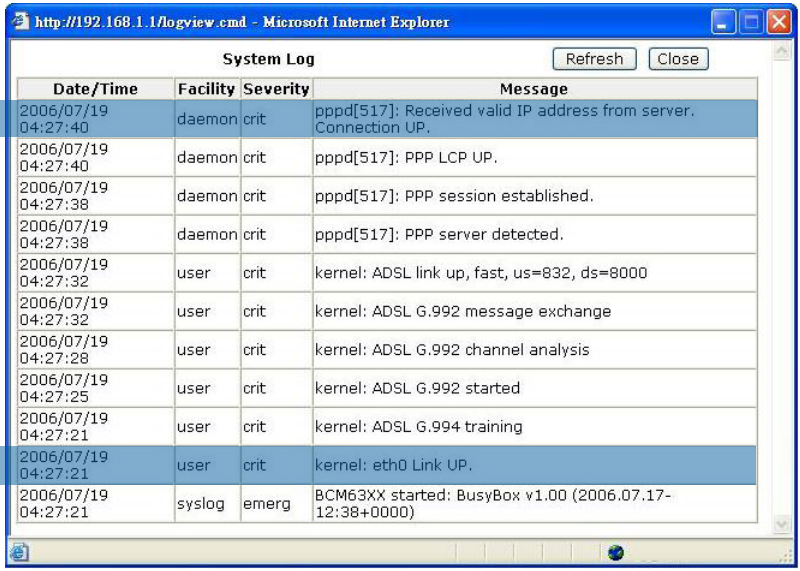
The **Date** and **Time** record the logging time. The **Priority** field shows the log level, the **Hostname** exhibits the position of the host, and the **Message** column displays the process the description of it before the colon is the name of the process and after the colon is the elaboration for that process.

For example, message 1 shows alert level information which is a kernel process containing detailed intrusion information; message 2 displays notice level information which is an IGMP process exhibiting that the IGMP function had been started.

Viewing System Log – Local Side (ADSL Router)


System Log
The System Log dialog allows you to view the System Log and configure the System Log options.
Click "View System Log" to view the System Log.
Click "Configure System Log" to configure the System Log options.
View System Log
Configure System Log

For viewing the system log on local side, click the **View System Log** button on the webpage for system log configuration.


http://192.168.1.1/logview.cmd - Microsoft Internet Explorer
System Log
Refresh
Close
Date/Time
Facility
Severity
Message
3
2006/07/19 04:27:40 daemon crit pppd[517]: Received valid IP address from server. Connection UP.
2006/07/19 04:27:40 daemon crit pppd[517]: PPP LCP UP.
2006/07/19 04:27:38 daemon crit pppd[517]: PPP session established.
2006/07/19 04:27:38 daemon crit pppd[517]: PPP server detected.
2006/07/19 04:27:32 user crit kernel: ADSL link up, fast, us=832, ds=8000
2006/07/19 04:27:32 user crit kernel: ADSL G.992 message exchange
2006/07/19 04:27:28 user crit kernel: ADSL G.992 channel analysis
2006/07/19 04:27:25 user crit kernel: ADSL G.992 started
2006/07/19 04:27:21 user crit kernel: ADSL G.994 training
4
2006/07/19 04:27:21 user crit kernel: eth0 Link UP.
2006/07/19 04:27:21 syslog emerg BCM63XX started: BusyBox v1.00 (2006.07.17-12:38+0000)

The system log record on the router will be displayed on a screen as shown above.

The **Date/Time** records the logging time, and the Facility field distinguishes different classes of system log message. The **Severity** field shows the log level, and the **Message** column displays the process and the description of it, the name of the process appears before the colon and the elaboration for that process after the colon.

For example, message 3 shows critical level information which is a pppd (PPP daemon) process showing that a valid IP address had been received from server, and connection is up; message 4 is a kernel process belonging to critical level information which reveals that the Ethernet 0 link is up.

You can press **Refresh** to update the log files or press **Close** to close the window.

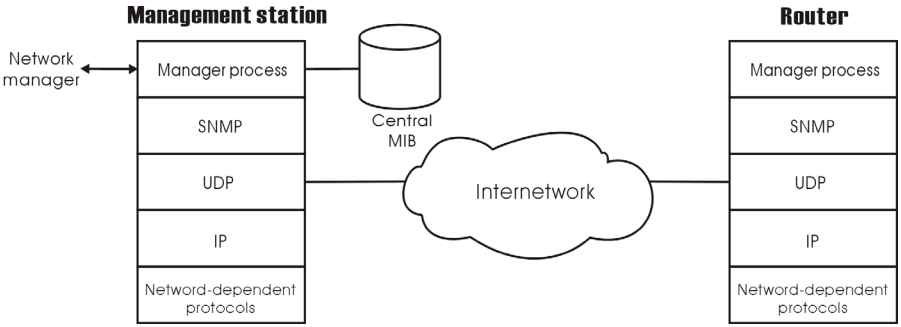
Note that the earlier messages may be automatically replaced by the updated information when the buffer is overflowed on the router.

SNMP Setting (NB6W and NB6Plus4W only)

SNMP, the abbreviation of Simple Network Management Protocol, is used to refer to a collection of specifications for network management that include the protocol itself, the definition of data structures and associated concepts.

A management station performs the **monitoring function** by retrieving the value of MIB objects. The management station and agents are linked by a network management protocol that is SNMP. The SNMP includes three key capabilities: **get**, **set** and **trap**. A single management station can handle many agents as long as SNMP remains relatively "simple", so the number can be high (hundreds or so).

The following picture is the typical configuration of protocols for SNMP. As for a stand-alone management station, a manager process controls access to a central MIB at the management station and provides an interface to the network manager. The manager process achieves network management by using SNMP, which will be implemented on top of the UDP, IP and the relevant network-dependent protocols (e.g., Ethernet).

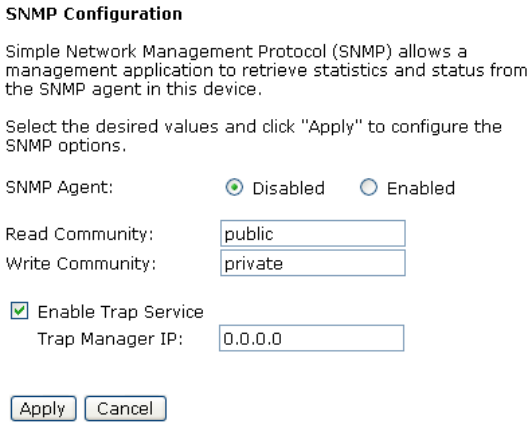


For an agent device that supports other applications, such as FTP, both TCP and UDP are required. An agent may issue a trap message in response to an event that affects the MIB and the underlying managed resources.

Note: There is no ongoing connection maintained between a management station and its agents. Instead, each exchange is a separate transaction between a management station and an agent.

Each agent is responsible for notifying the management station of any **unusual event**; for example, if the agent crashes and is rebooting, a link fails or an overload condition as defined by the packet load crosses some threshold. These events are communicated in SNMP messages known as **traps**.

Please select **SNMP** from the **Management** menu to make the following settings.



SNMP Agent:

Choose **Disable** to close this function; choose **Enabled** to open this function.

Read Community:

SNMP community for reading access only. The default setting is **public**. Please key in the data that your ISP provided.

Write Community:

SNMP community for reading and writing access. The default setting is **private**. Please key in the data that your ISP provided.

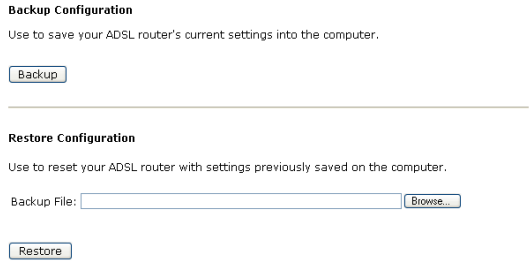
Enable Trap Service:

Configure the SNMP service to send a trap when it receives a request for information that does not contain the correct community name and does not match an accepted host name for the service. Check this box to enable this function, otherwise uncheck it.

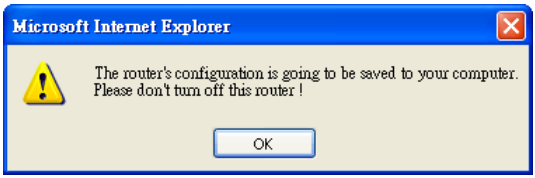
TRAP Manager IP:

Type an IP address as the remote workstation. If any abnormal condition happens, you can advice remote workstation through SNMP agent.

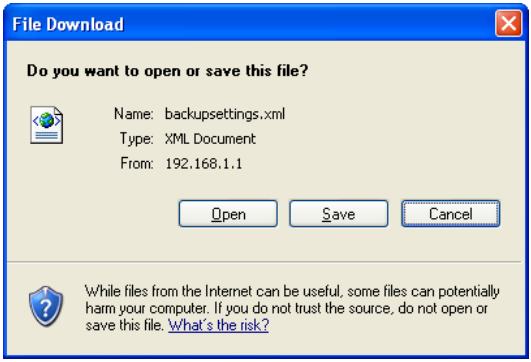
Backup Config


Backup Configuration
Use to save your ADSL router's current settings into the computer.
Backup
Restore Configuration
Use to reset your ADSL router with settings previously saved on the computer.
Backup File:
Browse...
Restore

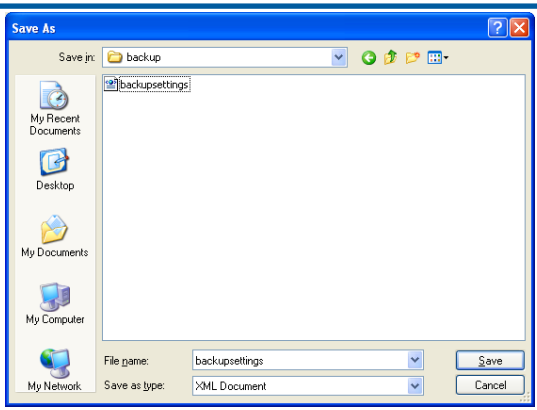
To backup your settings of the router, you can use **Backup Config** web page to save the configuration.


Microsoft Internet Explorer
The router's configuration is going to be saved to your computer.
Please don't turn off this router !
OK

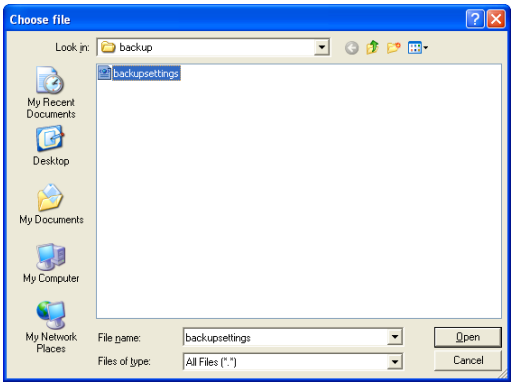
Click **Backup** button and the warning window will be prompted. Click **OK** to continue the backup procedure.


File Download
Do you want to open or save this file?
Name: backupsettings.xml
Type: XML Document
From: 192.168.1.1
Open
Save
Cancel
While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?

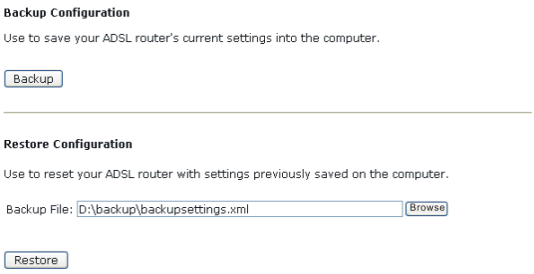
The system will ask your command about the next procedure. Click **Save** to backup.



You may change the file name and choose a place to save the backup file.

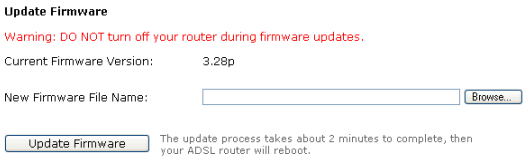


And when you want to restore the settings in the future, simply open **Backup Config** web page and use **Browse** button to locate the file.



After opening the backup file, click Restore.

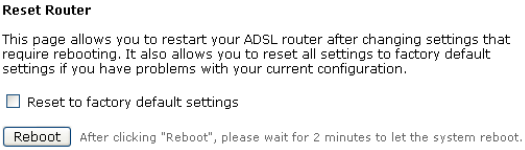
Update Firmware


Update Firmware
Warning: DO NOT turn off your router during firmware updates.
Current Firmware Version: 3.28p
New Firmware File Name:
Browse...
Update Firmware
The update process takes about 2 minutes to complete, then your ADSL router will reboot.

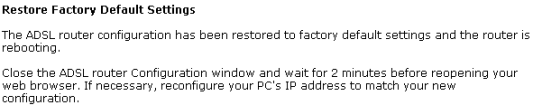
If you have to or want to update the firmware for this router, you can open the **Update Firmware** web page and choose the correct file by pressing **Browse**. Then click the **Update Firmware** button. The system will execute the update procedure automatically. When it is finished, the system will tell you the update is successfully.

Note: Router must not turn off during firmware updates.

Reset Router


Reset Router
This page allows you to restart your ADSL router after changing settings that require rebooting. It also allows you to reset all settings to factory default settings if you have problems with your current configuration.
Reset to factory default settings
Reboot
After clicking "Reboot", please wait for 2 minutes to let the system reboot.

To make the settings that you set for this router take effect, please open the **Reset Router** web page and click the **Reboot** button to invoke all settings.


Restore Factory Default Settings
The ADSL router configuration has been restored to factory default settings and the router is rebooting.
Close the ADSL router Configuration window and wait for 2 minutes before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

You can restore your web pages with default settings. Simply check **Reset to factory default settings** and click **Reboot.**

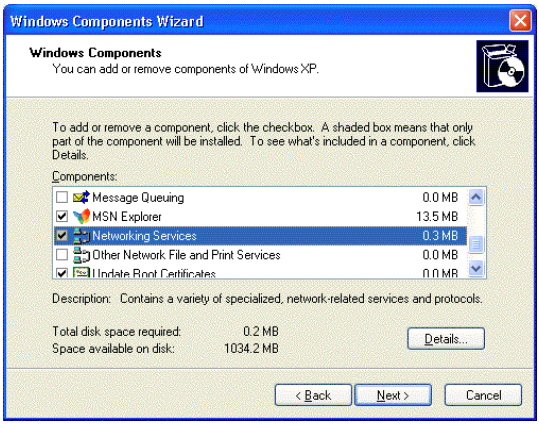
UPnP for XP

Universal plug and play (UPnP) is architecture for pervasive peer to peer network connectivity of intelligent appliances and PCs of all form factors. It is designed to bring easy-to-use, flexible, standards-based connectivity to ad-hoc or unmanaged networks whether in the home, in a small business, public places, or attached to the Internet.

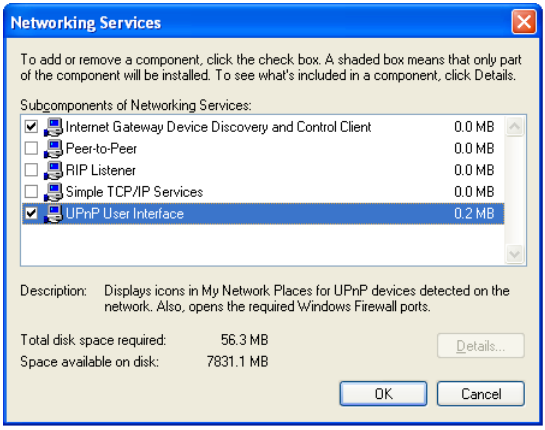
Only **Windows XP** supports UPnP function.

Please follow the steps below for installing UPnP components.

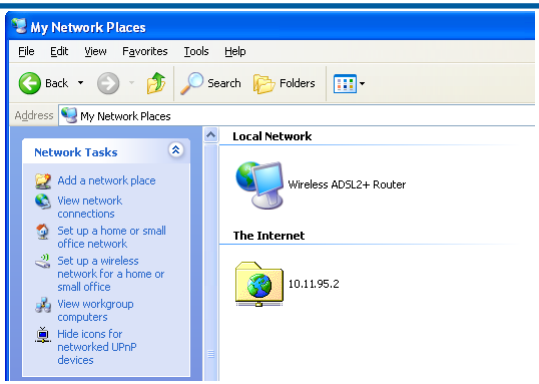
1. Click on the **Start** menu, point to **Settings** and click on **Control Panel**.


Windows Components Wizard
Windows Components
You can add or remove components of Windows XP.
To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
Message Queuing 0.0 MB
MSN Explorer 13.5 MB
Networking Services 0.3 MB
Other Network File and Print Services 0.0 MB
Update Root Certificates 0.0 MB
Description: Contains a variety of specialized, network-related services and protocols.
Total disk space required: 0.2 MB
Space available on disk: 1034.2 MB
Details...
< Back
Next >
Cancel

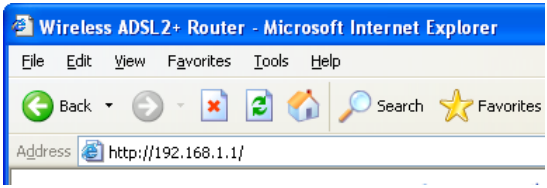
2. Select **Add or Remove Programs** > **Add/Remove Windows Components** to open **Windows Components Wizard** dialog box.


Networking Services
To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Subcomponents of Networking Services:
Internet Gateway Device Discovery and Control Client 0.0 MB
Peer-to-Peer 0.0 MB
RIP Listener 0.0 MB
Simple TCP/IP Services 0.0 MB
UPnP User Interface 0.2 MB
Description: Displays icons in My Network Places for UPnP devices detected on the network. Also, opens the required Windows Firewall ports.
Total disk space required: 56.3 MB
Space available on disk: 7831.1 MB
Details...
OK
Cancel

3. Select **Networking Services** and click **Details**. Click the **UPNP User Interface** check box.
4. Click **OK**. The system will install UPnP components automatically.


My Network Places
File Edit View Favorites Tools Help
Back Search Folders
Address My Network Places
Network Tasks
Add a network place
View network connections
Set up a home or small office network
Set up a wireless network for a home or small office
View workgroup computers
Hide icons for networked UPnP devices
Local Network
Wireless ADSL2+ Router
The Internet
10.11.95.2

5. After finishing the installation, go to **My Network Places**. You will find an icon (e.g., Wireless ADSL2+ Router) for UPnP function.


Wireless ADSL2+ Router - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.1.1/

6. Double click on the icon, and the ADSL router will open another web page via the port for UPnP function. The IE address will be directed to the configuration main webpage as shown in the graphic.
7. Now, the NAT traversal function has already been provided. The ADSL router will create a new virtual server automatically when the router detects that some internet applications is running on the PC.

CHAPTER 5: TROUBLESHOOTING

If the suggested solutions in this section do not resolve your issue, contact your system administrator or Internet service provider.

Problems with LAN

PCs on the LAN cannot get IP addresses from the ADSL Router.

The chances are that the interface used as DHCP server is modified and the client PCs do not renew IP addresses.

If your DHCP server is enabled on Private IP Address previously and you modify the interface to Public IP Address, the client PCs should renew IP addresses.

The PC on the LAN cannot access the Web page of the ADSL Router.

Check that your PC is on the same subnet with the ADSL Router.

Problems with WAN

You cannot access the Internet.

- Check the physical connection between the ADSL Router and the LAN.

  If the LAN LED on the front panel is off or keeps blinking, there may be problem on the cable connecting to the ADSL Router.

  At the DOS prompt, ping the IP address of the ADSL Router, e.g., ping 192.168.1.1. If the following response occurs:

  Reply from 192.168.1.1: bytes=32 time=100ms TTL=253

  Then the connection between the ADSL Router and the network is OK.

  If you get a failed ping with the response of:

  Request timed out

  Then the connection is fail. Check the cable between the ADSL Router and the network.

- Check the DNS setting of the ADSL Router.

  At the DOS prompt, ping the IP addresses of the DNS provided by your ISP. For example, if your DNS IP is 168.95.1.1, then ping 168.95.1.1. If the following response occurs:

  Reply from 168.95.1.1: bytes=32 time=100ms TTL=253

  Then the connection to the DNS is OK.

  If you get a failed ping with the response of:

  Request timed out

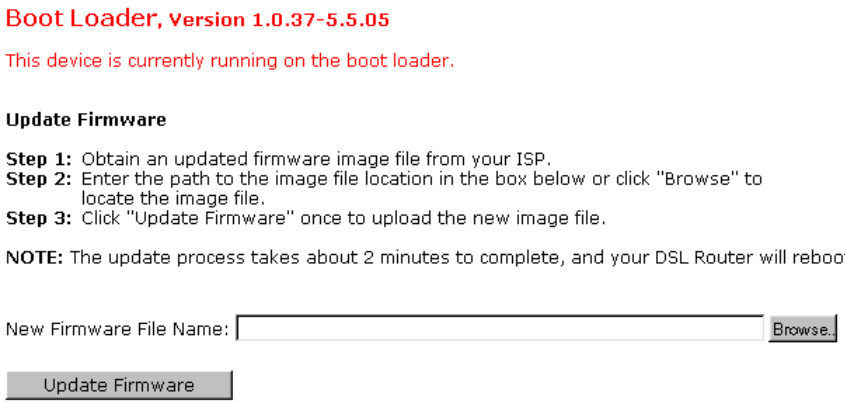
  Then the DNS is not reachable. Check your DNS setting on the ADSL Router.

Problems with Upgrading

The following lists the error messages that you may see during upgrading and the action to take.

- Error message: All the ADSL LEDs light up and cannot light off as usual.

  Possible cause: When users are executing firmware upgrade and saving settings to the router, the power for the router is lost for some unknown reasons, the normal web page for the router might be damaged. After power on your router, the LEDs might not work normally.


Boot Loader, Version 1.0.37-5.5.05
This device is currently running on the boot loader.
Update Firmware
Step 1: Obtain an updated firmware image file from your ISP.
Step 2: Enter the path to the image file location in the box below or click "Browse" to locate the image file.
Step 3: Click "Update Firmware" once to upload the new image file.
NOTE: The update process takes about 2 minutes to complete, and your DSL Router will reboot.
New Firmware File Name:
Browse...
Update Firmware

  Action: Setup you PC with a static IP address, such as 192.168.1.2, and then access the router's web page by entering http://192.168.1.1. Then update the firmware again.

- Error Message: Image uploading failed. The selected file contains an illegal image.

  Possible cause: The firmware file format is invalid.

  Action: Check to see whether the file format is correct; otherwise download a firmware file with correct format.

- Error Message: Image uploading failed. The system is out of memory.

  Possible cause: It may be caused by the lack of memory.

  Action: Reboot your ADSL Router and perform the upgrade task again.

- Error Message: Image uploading failed. No image file was selected.

  Possible cause: You did not select a file correctly.

  Action: Download a compatible firmware from the web.

CHAPTER 6: GLOSSARY

ARP (Address Resolution Protocol)

ARP is a TCP/IP protocol for mapping an IP address to a physical machine address that is recognized in the local network, such as an Ethernet address.

A host wishing to obtain a physical address broadcasts an ARP request onto the TCP/IP network. The host on the network that has the IP address in the request then replies with its physical hardware address.

Inverse ARP (In-ARP), on the other hand, is used by a host to discover its IP address. In this case, the host broadcasts its physical address and a RARP server replies with the host's IP address.

DHCP (Dynamic Host Configuration Protocol)

When operates as a DHCP server, the ADSL Router assign IP addresses to the client PCs on the LAN. The client PCs "leases" these Private IP addresses for a user-defined amount of time. After the lease time expires, the private IP address is made available for assigning to other network devices.

The DHCP IP address can be a single, fixed public IP address, an ISP assigned public IP address, or a private IP address.

If you enable DHCP server on a private IP address, a public IP address will have to be assigned to the NAT IP address, and NAT has to be enabled so that the DHCP IP address can be translated into a public IP address. By this, the client PCs are able to access the Internet.

LAN (Local Area Network) & WAN (Wide Area Network)

A LAN is a computer network limited to the immediate area, usually the same building or floor of a building. A WAN, on the other hand, is an outside connection to another network or the Internet.

The Ethernet side of the ADSL Router is called the LAN port. It is a twisted-pair Ethernet 10Base-T interface. A hub can be connected to the LAN port. More than one computers, such as server or printer, can be connected through this hub to the ADSL Router and composes a LAN.

The DSL port of the ADSL Router composes the WAN interface, which supports PPP or RFC 1483 connecting to another remote DSL device.

NAT (Network Address Translation) IP Address

NAT is an Internet standard that translates a private IP within one network to a public IP address, either a static or dynamic one. NAT provides a type of firewall by hiding internal IP addresses. It also enables a company to use more internal IP addresses.

If the IP addresses given by your ISP are not enough for each PC on the LAN and the ADSL Router, you need to use NAT. With NAT, you make up a private IP network for the LAN and assign an IP address from that network to each PC. One of some public addresses is configured and mapped to a private workstation address when accesses are made through the gateway to a public network.

For example, the ADSL Router is assigned with the public IP address of 168.111.2.1. With NAT enabled, it creates a Virtual LAN. Each PC on the Virtual LAN is assigned with a private IP address with default value of 192.168.2.2 to 192.168.2.254. These PCs are not accessible by the outside world but they can communicate with the outside world through the public IP 168.111.2.1.

Private IP Address

Private IP addresses are also LAN IP addresses, but are considered "illegal" IP addresses to the Internet. They are private to an enterprise while still permitting full network layer connectivity between all hosts inside an enterprise as well as all public hosts of different enterprises.

The ADSL Router uses private IP addresses by assigning them to the LAN that cannot be directly accessed by the Internet or remote server. To access the Internet, private network should have an agent to translate the private IP address to public IP address.

Public IP Address

Public IP addresses are LAN IP addresses that can be considered "legal" for the Internet, because they can be recognized and accessed by any device on the other side of the DSL connection. In most cases they are allocated by your ISP.

If you are given a range of fixed IP addresses, then one can be assigned to the router and the others to network devices on the LAN, such as computer workstations, ftp servers, and web servers.

PVC (Permanent Virtual Circuit)

A PVC is a logical point-to-point circuit between customer sites. PVCs are low-delay circuits because routing decisions do not need to be made along the way. Permanent means that the circuit is preprogrammed by the carrier as a path through the network. It does not need to be set up or turned down for each session.

RIP (Routing Information Protocol)

RIP is a routing protocol that uses the distance-vector routing algorithms to calculate least-hops routes to a destination. It is used on the Internet and is common in the NetWare environment. It exchanges routing information with other routers. It includes V1, V2 and V1&V2, which controls the sending and receiving of RIP packets over Ethernet.

UDP (User Datagram Protocol)

UDP is a connectionless transport service that dispenses with the reliability services provided by TCP. UDP gives applications a direct interface with IP and the ability to address a particular application process running on a host via a port number without setting up a connection session.

Virtual Server

You can designate virtual servers, e.g., a FTP, web, telnet or mail server, on your local network and make them accessible to the outside world. A virtual server means that it is not a dedicated server -- that is, the entire computer is not dedicated to running on the public network but in the private network.

VPI (Virtual Path Identifier) & VCI (Virtual Channel Identifier)

A VPI is a 8-bit field while VCI is a 16-bit field in the ATM cell header. A VPI identifies a link formed by a virtual path and a VCI identifies a channel within a virtual path. In this way, the cells belonging to the same connection can be distinguished. A unique and separate VPI/VCI identifier is assigned in advance to indicate which type of cell is following, unassigned cells, physical layer OAM cells, metasignaling channel or a generic broadcast signaling channel. Your ISP should supply you with the values.

APPENDIX A: CLIENT SETUP FOR 802.1X, WPA, AND WPA-PSK

Retreiving Client Certificate

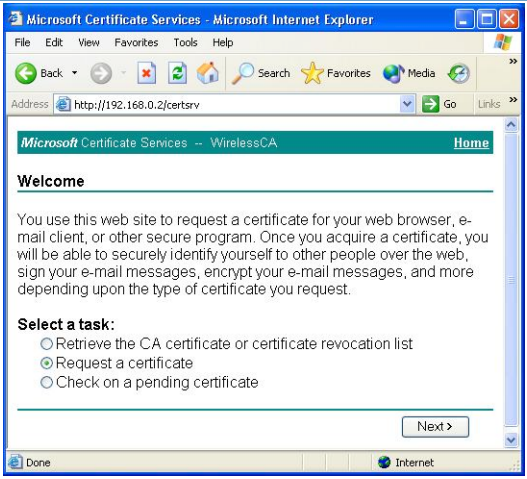
- This step is only required if you intend to authenticate with EAP/TLS.

  While there are many ways you may receive a certificate from your Certificate Authority, the example here is to show you how to retrieve your certificate from a Microsoft Certificate Services server via its easy web interface.

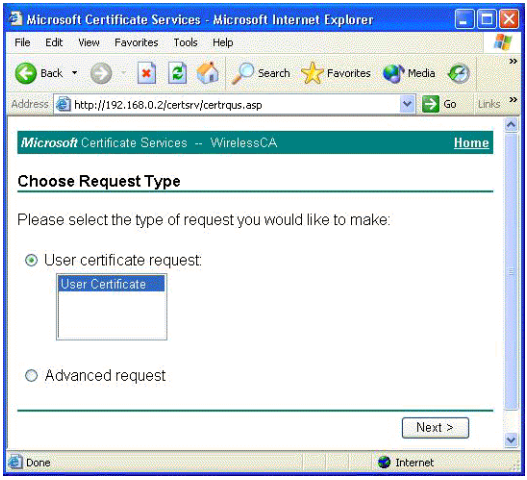
1. Please connect the client to a network that doesn't require port authentictaion.
2. Open up Microsoft Explorer, connect to your CA via the url http://yourserver/certsrv (see your local administrator if it has been changed from the default).

   For example, if the Microsoft Certificate Service server uses the IP address 192.168.0.2, then we have to key in http://192.168.0.2/certsrv on the url box.

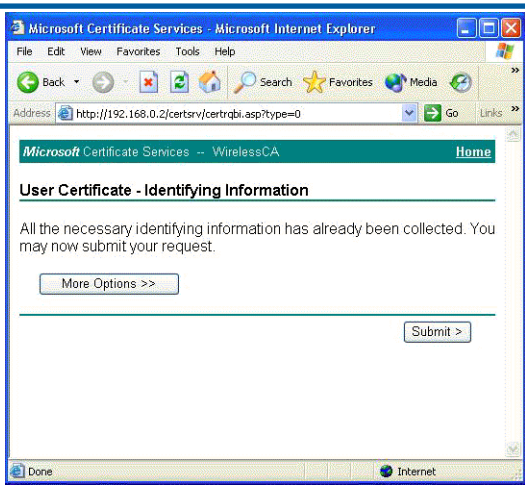
3. You will be asked to log in, use your domain credentials. (e.g., ABC)


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.0.2/certsrv
Go Links
Microsoft Certificate Services -- WirelessCA
Home
Welcome
You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.
Select a task:
Retrieve the CA certificate or certificate revocation list
Request a certificate
Check on a pending certificate
Next >
Done
Internet

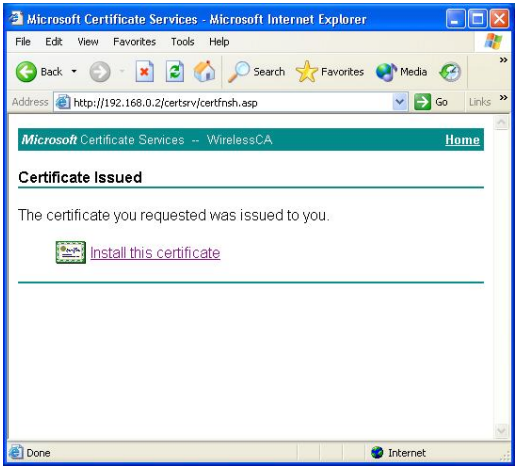
4. Make sure that Request a certificate is selected, and click Next.



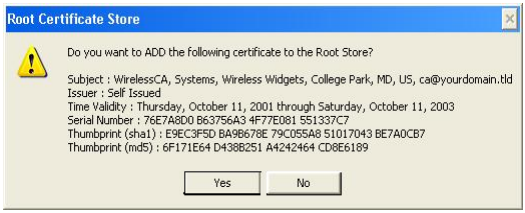
5. Select User Certificate, then Next.


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.0.2/certsrv/certrqbi.asp?type=0
Go Links
Microsoft Certificate Services -- WirelessCA
Home
User Certificate - Identifying Information
All the necessary identifying information has already been collected. You may now submit your request.
More Options >>
Submit >
Done
Internet

6. Click Submit.

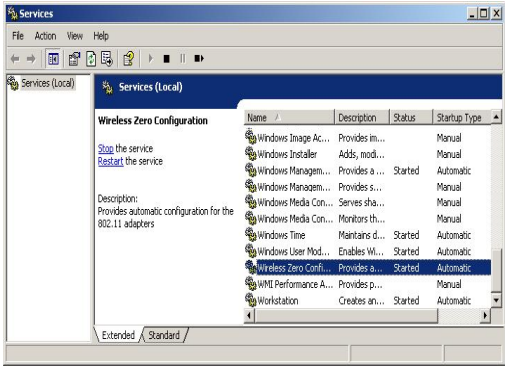


7. You may retrieve your certificate by clicking Install this certificate.

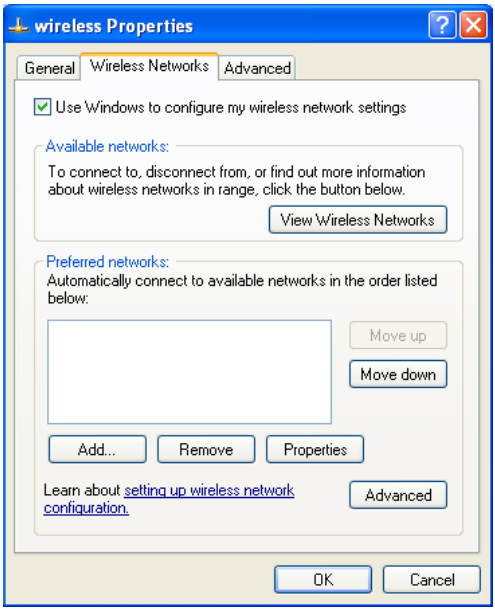

Root Certificate Store
Do you want to ADD the following certificate to the Root Store?
Subject : WirelessCA, Systems, Wireless Widgets, College Park, MD, US, ca@yourdomain.tld
Issuer : Self Issued
Time Validity : Thursday, October 11, 2001 through Saturday, October 11, 2003
Serial Number : 76E7A8D0 B63756A3 4F77E081 551337C7
Thumbprint (sha1) : E9EC3F5D BA9B678E 79C055A8 51017043 BE7A0CB7
Thumbprint (md5) : 6F171E64 D438B251 A4242464 CD8E6189
Yes
No

8. You'll receive a confirmation message about accepting the certificate, click Yes

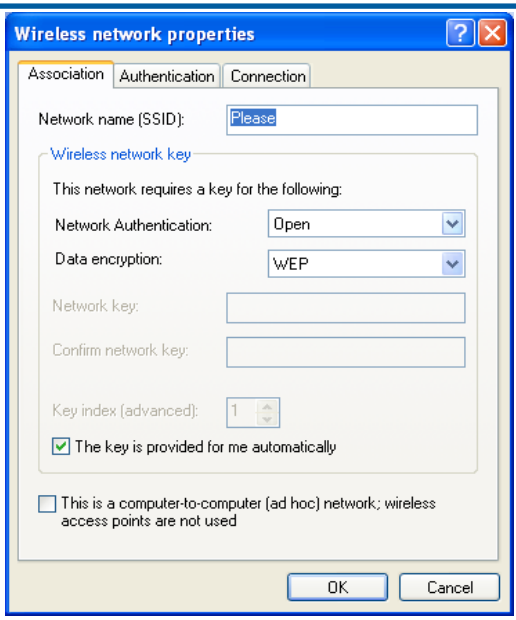
Enabling 802.1x Authentication and Security



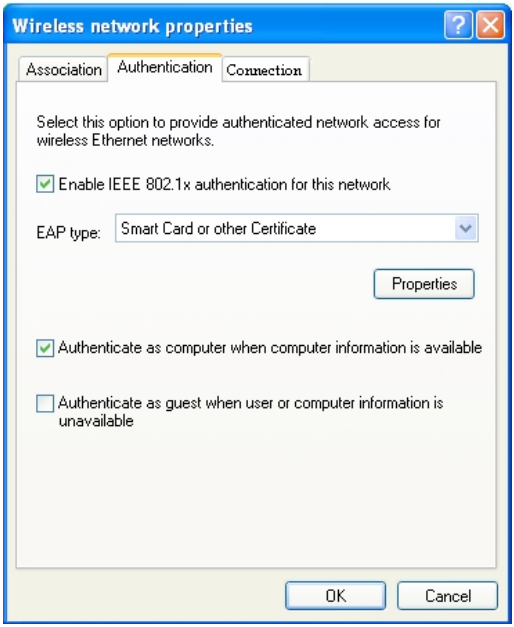
1. Click **Run** from the **Start** menu. Type services.msc and click **OK**.
2. Scroll to the bottom of the list. Double click on the **Wireless Zero Configuration** service and verify that it is set to Automatic and that it is Started. Click **OK** to continue.



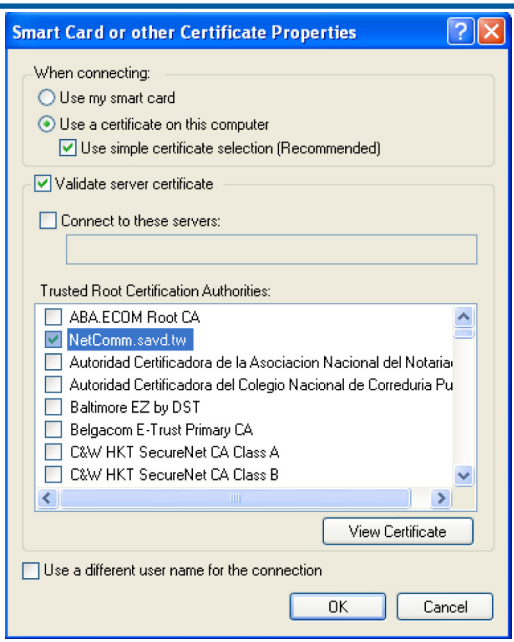
3. Click the **Start** button, select **Control Panel**, then **Network Connections**.
4. Right click on your wireless network card and select **Properties**. Click on the **Wireless Networks** tab.
5. Click **Add** to continue.



6. Select the **Association** Tab, and enter the SSID of the AP. (e.g., Please)
7. Set Open as the **Network Authentication** from the drop down menu, and WEP for **Data encryption.**
8. Click **OK**, and then select the **Authentication** Tab.


Wireless network properties
Association
Authentication
Connection
Select this option to provide authenticated network access for wireless Ethernet networks.
Enable IEEE 802.1x authentication for this network
EAP type:
Smart Card or other Certificate
Properties
Authenticate as computer when computer information is available
Authenticate as guest when user or computer information is unavailable
OK
Cancel

9. Ensure that **Enable network access control using IEEE 802.1X** is selected, and **Smart Card or other Certificate** is selected from the EAP type.
10. Click **Properties** under **EAP** type.

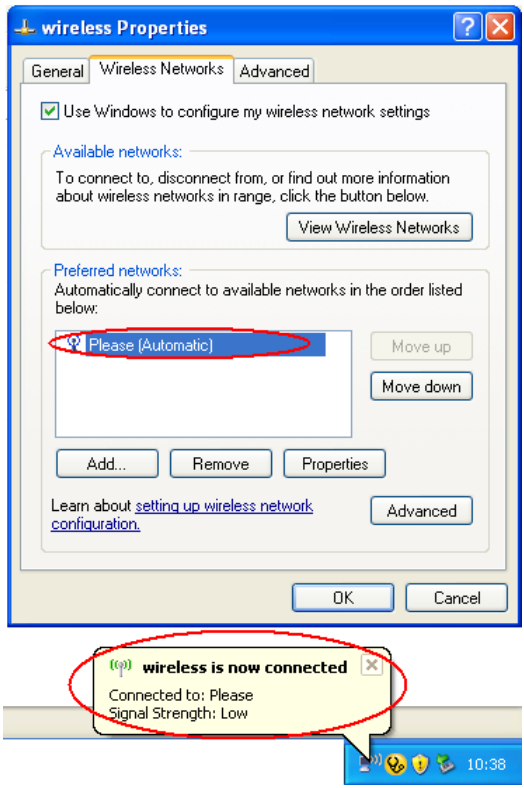

Smart Card or other Certificate Properties
When connecting:
Use my smart card
Use a certificate on this computer
Use simple certificate selection (Recommended)
Validate server certificate
Connect to these servers:
Trusted Root Certification Authorities:
ABA.ECOM Root CA
NetComm.savd.tw
Autoridad Certificadora de la Asociacion Nacional del Notaria
Autoridad Certificadora del Colegio Nacional de Correduria Pu
Baltimore EZ by DST
Belgacom E-Trust Primary CA
C&W HKT SecureNet CA Class A
C&W HKT SecureNet CA Class B
View Certificate
Use a different user name for the connection
OK
Cancel

11. You can choose whether to use one of your certificates you have loaded on the computer, or use a smart card for access.

    In our example, Use a certificate on this computer option is chose and Use simple certificate selection (Recommended) is checked.

12. Check the **Validate server certificate** check box if server certificate validation is required.
13. In the **Trusted Root Certification Authorities** field, check the check box beside the name of the certificate authority from which the server certificate was downloaded. (e.g., NetComm.savd.tw)

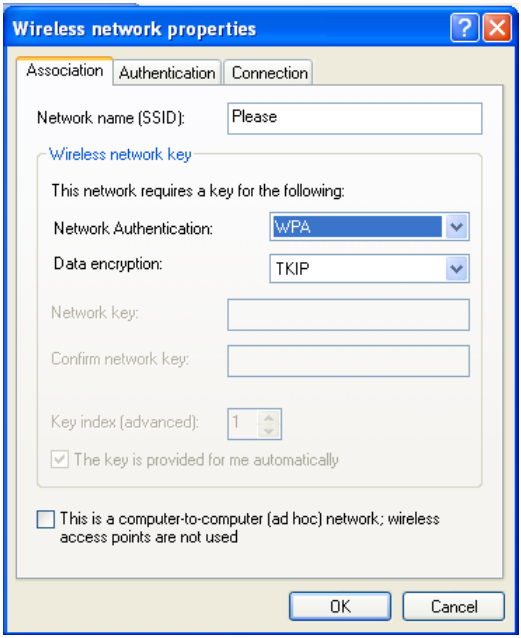
    Note that if you leave all check boxes unchecked, you will be prompted to accept a connection to the root certification authority during the authentication process.



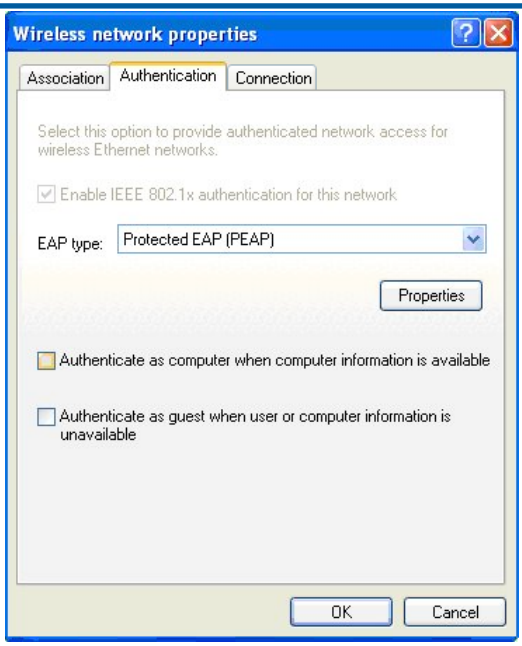
14. Click **OK** twice to close the dialogs until return to **Wireless Networks** tab of **wireless properties**. Now we can see the wireless network which we have just set up being displayed on the **Prefered networks**.
15. Click **OK** to save your settings. The configuration is complete

Enabling WPA Authentication and Security

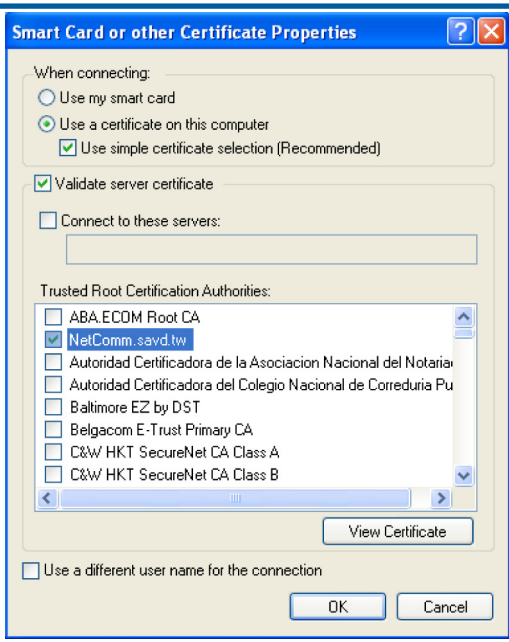
The first four steps are the same as the setting for 802.1x authentication, please refer to the previous part.



5. Select the **Association** Tab, and enter the SSID of the AP. (e.g., Please)
6. Choose WPA from the drop down menu for the **Network Authentication**, and TKIP for **Data encryption.**
7. Click **OK**, and then select the **Authentication** Tab.

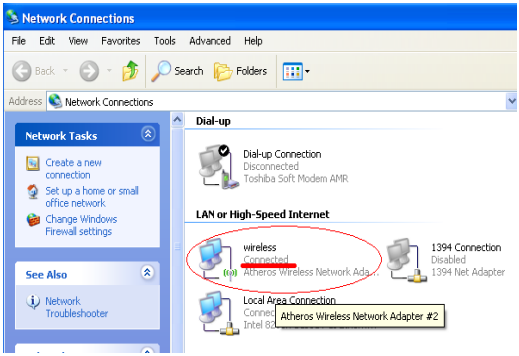


8. The **Enable network access control using IEEE 802.1X** is selected by default, and **Protected EAP (PEAP)** is selected from the EAP type.
9. Click **Properties** under **EAP type**.


Smart Card or other Certificate Properties
When connecting:
Use my smart card
Use a certificate on this computer
Use simple certificate selection (Recommended)
Validate server certificate
Connect to these servers:
Trusted Root Certification Authorities:
ABA.ECOM Root CA
NetComm.savd.tw
Autoridad Certificadora de la Asociacion Nacional del Notaria
Autoridad Certificadora del Colegio Nacional de Correduria Pu
Baltimore EZ by DST
Belgacom E-Trust Primary CA
C&W HKT SecureNet CA Class A
C&W HKT SecureNet CA Class B
View Certificate
Use a different user name for the connection
OK
Cancel

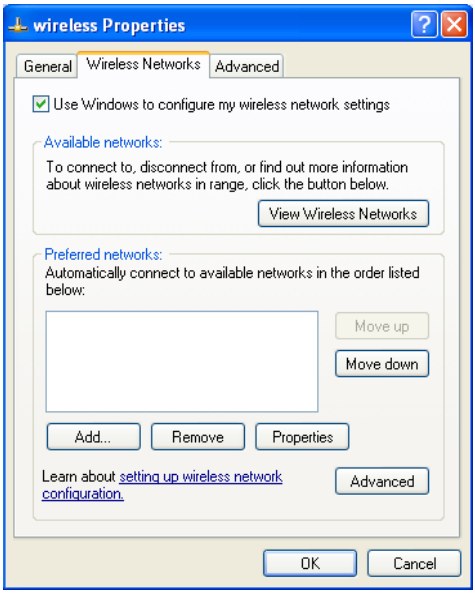
10. Choose **Use a certificate on this computer** option and select **Use simple certificate selection (Recommended)**.
11. Check the **Validate server certificate** check box if server certificate validation is required
12. In the **Trusted Root Certification Authorities** field, check the check box beside the name of the certificate authority from which the server certificate was downloaded. (e.g., NetComm.savd.tw)

    Note that if you leave all check boxes unchecked, you will be prompted to accept a connection to the root certification authority during the authentication process.

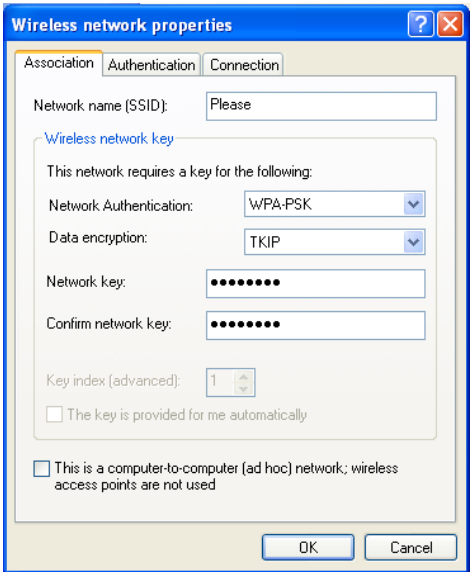


13. Click **OK** three times to close the dialogs and save all the settings until return to **Network Connections**.
14. Now the configuration for WPA authentication is completed. And you may start to use the wireless device.

Enabling WPA-PSK Authentication and Security

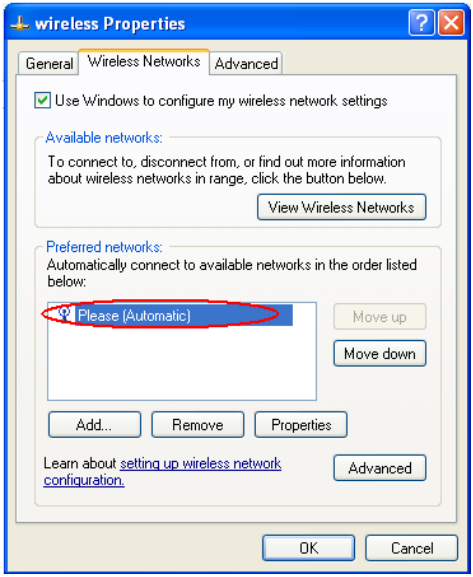


1. Click the **Start** button, select **Control Panel**, then **Network Connections**.
2. Right click on your wireless network card and select **Properties**. Click on the **Wireless Networks** tab.
3. Click **Add** to continue.

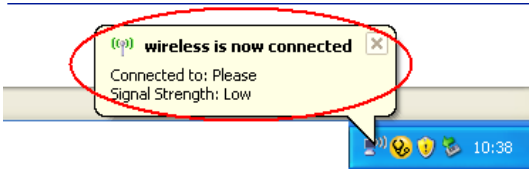


4. Select the **Association** Tab, and enter the SSID of the AP. (e.g., Please)

5. Choose WPA-PSK for the **Network Authentication** and TKIP for **Data encryption.**
6. Enter **Network key** twice to access the AP.
7. Click **OK** to save the settings and return to the **Wireless Networks** tab on **Wireless Properties**.



8. The Network with WPA-PSK authentication has been set up, and is displayed in the preferred networks field.



9. Now the configuration for WPA-PSK authentication is completed.

APPENDIX B: LEGAL & REGULATORY INFORMATION

This manual is copyright. Apart from any fair dealing for the purposes of private study, research, criticism or review, as permitted under the Copyright Act, no part may be reproduced, stored in a retrieval system or transmitted in any form, by any means, be it electronic, mechanical, recording or otherwise, without the prior written permission of NetComm Limited. NetComm Limited accepts no liability or responsibility, for consequences arising from the use of this product.

NetComm Limited reserves the right to change the specifications and operating details of this product without notice.

NetComm is a registered trademark of NetComm Limited.

All other trademarks are acknowledged the property of their respective owners.

Customer Information

ACA (Australian Communications Authority) requires you to be aware of the following information and warnings:

(1) This unit shall be connected to the Telecommunication Network through a line cord which meets the requirements of the ACA TS008 Standard.

(2) This equipment has been tested and found to comply with the Standards for C-Tick and or A-Tick as set by the ACA . These standards are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio noise and, if not installed and used in accordance with the instructions detailed within this manual, may cause interference to radio communications. However, there is no guarantee that interference will not occur with the installation of this product in your home or office. If this equipment does cause some degree of interference to radio or television reception, which can be determined by turning the equipment off and on, we encourage the user to try to correct the interference by one or more of the following measures:

- Change the direction or relocate the receiving antenna.
- Increase the separation between this equipment and the receiver.
- Connect the equipment to an alternate power outlet on a different power circuit from that to which the receiver/TV is connected.
- Consult an experienced radio/TV technician for help.

(3) The power supply that is provided with this unit is only intended for use with this product. Do not use this power supply with any other product or do not use any other power supply that is not approved for use with this product by NetComm. Failure to do so may cause damage to this product, fire or result in personal injury.

Product Warranty

The warranty is granted on the following conditions:

1. This warranty extends to the original purchaser (you) and is not transferable;
2. This warranty shall not apply to software programs, batteries, power supplies, cables or other accessories supplied in or with the product;
3. The customer complies with all of the terms of any relevant agreement with NetComm and any other reasonable requirements of NetComm including producing such evidence of purchase as NetComm may require;
4. The cost of transporting product to and from NetComm's nominated premises is your responsibility; and,
5. NetComm does not have any liability or responsibility under this warranty where any cost, loss, injury or damage of any kind, whether direct, indirect, consequential, incidental or otherwise arises out of events beyond NetComm's reasonable control. This includes but is not limited to: acts of God, war, riot, embargoes, acts of civil or military authorities, fire, floods, electricity outages, lightning, power surges, or shortages of materials or labour.
6. The customer is responsible for the security of their computer and network at all times. Security features may be disabled within the factory default settings. NetComm recommends that you enable these features to enhance your security.

The warranty is automatically voided if:

1. You, or someone else, use the product, or attempts to use it, other than as specified by NetComm;
2. The fault or defect in your product is the result of a voltage surge subjected to the product either by the way of power supply or communication line, whether caused by thunderstorm activity or any other cause(s);
3. The fault is the result of accidental damage or damage in transit, including but not limited to liquid spillage;
4. Your product has been used for any purposes other than that for which it is sold, or in any way other than in strict accordance with the user manual supplied;
5. Your product has been repaired or modified or attempted to be repaired or modified, other than by a qualified person at a service centre authorised by NetComm; and,
6. The serial number has been defaced or altered in any way or if the serial number plate has been removed.

Limitations of Warranty

The Trade Practices Act 1974 and corresponding State and Territory Fair Trading Acts or legalisation of another Government ("the relevant acts") in certain circumstances imply mandatory conditions and warranties which cannot be excluded. This warranty is in addition to and not in replacement for such conditions and warranties.

To the extent permitted by the Relevant Acts, in relation to your product and any other materials provided with the product ("the Goods") the liability of NetComm under the Relevant Acts is limited at the option of NetComm to:

- Replacement of the Goods; or
- Repair of the Goods; or
- Payment of the cost of replacing the Goods; or
- Payment of the cost of having the Goods repaired.

All NetComm ACN 002 490 486 products have a standard 12 months warranty from date of purchase. However some products have an extended warranty option (refer to packaging). To be eligible for the extended warranty you must supply the requested warranty information to NetComm within 30 days of the original purchase by registering on-line via the NetComm web site at

www.netcomm.com.au

NetComm®
www.netcomm.com.au

NetComm Limited ABN 85 002 490 486
PO Box 1200, Lane Cove NSW 2066 Australia
E – sales@netcomm.com.au **W** – www.netcomm.com.au